Markus Reijonen

Lukitusjärjestelmän eheyden tason tutkimus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikan tutkinto-ohjelma

Insinöörityö

11.1.2022

Tiivistelmä

Tekijä:	Markus Reijonen
Otsikko:	Lukitusjärjestelmän eheyden tason tutkimus
Sivumäärä:	56 sivua + 8 liitettä
Aika:	11.1.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Automaatiotekniikka
Ohjaajat:	Lehtori Kristian Junno Tehdasinsinööri Ville Hakkarainen

---

Insinöörityön tavoitteena oli selvittää, mitä turvajärjestelmällä toteutettavia turvatoimintovaatimuksia oli tunnistettu prosessin riskinarvioinnissa ja mitkä niiden turvallisuuden eheyden tason vaatimukset olivat. Lisäksi oli tarkoitus selvittää lukitusjärjestelmän kykenevyys täyttää sille asetetut turvajärjestelmävaatimukset. Tavoitteena oli tämän pohjalta antaa suosituksia, kuinka tulisi edetä turva-automaatiojärjestelmän toteutusprojektin aloituksessa, mikäli siihen päätettäisiin ryhtyä.

Insinöörityön aikana tutkittiin tehtaan lukitusjärjestelmää turva-automaatiojärjestelmän elinkaarimallin ensimmäisten osioiden kautta riskinarvioinnista suunnitteluun. Tutkinnan kohteena olivat tehtaan riskinarviointi, siinä tunnistetut turvatoimintovaateet ja niiden käytännön toteutus lukitusjärjestelmän avulla. Lukitusjärjestelmästä tutkittiin myös sen arkkitehtuuria ja erillisyyttä käyttöautomaatiojärjestelmästä.

Insinöörityön lopputuloksena saatiin kuva käytössä olevan lukitusjärjestelmän kykenevyydestä täyttää nykyisen muotoisen turva-automaatiojärjestelmän vaatimukset. Lisäksi saatiin aikaan lista asioista, joita tulee tehdä ja päättää ennen varsinaista turva-automaatiojärjestelmän toteutusprojektia. Insinöörityön lopputuloksena insinöörityön tilaaja saa kuvan tulevan projektin työn laajuudesta.

Avainsanat: toiminnallinen turvallisuus, turva-automaatiojärjestelmä, turvallisuuden eheyden taso, riskinarviointi

Abstract

Author:	Markus Reijonen
Title:	Safety Interlock System Integrity Level Study
Number of Pages:	56 pages + 8 appendices
Date:	11 January 2022
Degree:	Bachelor of Engineering
Degree Programme:	Degree Programme in Electrical and Automation Engineering
Professional Major:	Automation engineering
Supervisors:	Kristian Junno, Senior Lecturer Ville Hakkarainen, Plant Engineer

---

The objective of the Thesis work was to find out what safety functions to be implemented with the current safety interlock system had been identified in the process risk assessment and what were the requirements for their Safety Integrity Levels. Another objective was to determine the ability of the current safety interlock system to meet the requirements imposed on it by modern Safety Instrumented Systems. Based on this, the purpose was to make recommendations on how to proceed with the start of the Safety Instrumented System implementation project, and whether to undertake it.

During the Thesis work, the safety interlock system was studied through the first parts of the Safety Instrumented System Lifecycle model from risk assessment to design. The subject of this investigation was the plant's risk assessment, the safety function requirements identified in it and their implementation in the safety interlock system. The safety interlock system was also studied for its architecture and separation from the Basic Process Control System.

The result shows the ability of the current safety interlock system to meet the requirements set for modern Safety Instrumented Systems. In addition, a list of matters to be done and decided upon before the beginning of design project of the Safety Instrumented System was provided. As a result, the client has better understanding of the scope of the work of the future project.

Keywords: Functional safety, Safety Instrumented System, Safety Integrity Level, Risk Assessment Analysis

Sisällys

Lyhenteet

1 Johdanto 1

2 Turva-automaatiojärjestelmiä koskevia määräyksiä 4

2.1 Direktiivit, lait ja valtioneuvoston asetukset 4
2.2 Standardit 6

3 Turva-automaatiojärjestelmä 8

3.1 Fyysinen rakenne 9
3.2 Vikaantuminen 10

4 Elinkaarimalli 13

4.1 Vaaran ja riskin arviointi 13
4.1.1 Suojauskerrokset 15
4.1.2 HAZOP-tarkastelu 16
4.2 Turvatoimintojen kohdentaminen suojauskerroksille 18
4.2.1 LOPA-menettely 18
4.3 Turva-automaatiojärjestelmän turvallisuusvaatimusten erittely 26
4.3.1 Turvallisuuden eheys ja turvallisuuden eheyden taso 27
4.3.2 Äänestysrakenne ja vikasietoisuus 28
4.3.3 Systemaattinen kyvykkyys 34
4.4 Turva-automaatiojärjestelmän suunnittelu 34
4.4.1 Turva-automaatiojärjestelmän erillisyys 37
4.5 Muut elinkaarimallin tasot 37
4.5.1 Turva-automaatiojärjestelmän asennus, käyttöönotto ja kelpuutus 38
4.5.2 Turva-automaatiojärjestelmän käyttö, ylläpito ja muutokset 38
4.5.3 Käytöstä poisto 39

5 INEOS Composites Finland Oy:n turvajärjestelmä 40

5.1 Selvityksen suorituksen kuvaus 40
5.2 Laitoksen riskinarviointi 42
5.3 Käytössä oleva turvajärjestelmä 44
5.3.1 Logiikkaosa 45

5.3.2 Kenttälaitteet 46
5.3.3 Esimerkkipiiri 47
5.4 Esimerkkipiirin turvallisuuden eheyden taso ja vikasietoisuus 51
5.4.1 Turvajärjestelmän erillisyys 52

6 Yhteenveto 53

Lähteet 57

Liitteet
Liite 1: Riskinarviointi: Korkea paine reaktorilla DC-81601
Liite 2: Lukitusdokumentti
Liite 3: Kojeluettelo: PSA-81605
Liite 4: Kojeluettelo: TICA-81601
Liite 5: Kojeluettelo: TZ-81659
Liite 6: Kojeluettelo: XCV-816103
Liite 7: Esimerkkipiirin lukitusjärjestelmän virtapiirikaaviot
Liite 8: Yksinkertaistus liitteestä 7

Lyhenteet

ATEX *Atmosphères Explosibles*. Räjähdysvaarallisissa tiloissa käytettäviä laitteita koskeva lainsäädäntö ja standardisointi.

EMC *Electromagnetic Compatibility*. Tarkoittaa elektronisen laitteen tai järjestelmän kykyä toimia luotettavasti luonnollisessa toimintaympäristössään.

EU *Euroopan Unioni*. Vuonna 1992 Maastrichtissa sopimuksella Euroopan unionista perustettu, nykyään 27 eurooppalaisen jäsenvaltion muodostama taloudellinen ja poliittinen liitto.

HAZOP *Hazard and Operability.* Vaara- ja käytettävyystarkastelulla yksilöidään ja arvioidaan prosessilaitoksessa olevia vaaroja.

HFT *Hardware Fault Tolerance*. Järjestelmän vikasietoisuus kertoo kuinka monta yhtäaikaista vaarallista vikaantumista turvatoiminto sietää turvatoiminnon toimintakyky säilyttäen.

IEC *International Electrotechical Comission*. Kansainvälinen sähköalan standardointiorganisaatio, jonka jäseninä ovat kansalliset järjestöt

LOPA *Layer Of Protection Analysis*. Suojauskerrosanalyysillä analysoidaan vaaroja, jotta voidaan päättää, tarvitaanko turva-automaatiotoimintoja. Lisäksi määritellään jokaiselle turva-automaatiotoiminnolle vaadittava turvallisuuden eheyden taso.

MTTR *Mean Time To Recovery*. Keskimääräinen korjausaika tarkoittaa korjauksiin käytetyn kokonaisajan ja korjausmäärien suhdetta. Aika lasketaan vian havaitsemisesta sen korjaukseen ja takaisin käyttöön saamiseen.

PFD_{avg} *Probability to Fail on Demand average*. Komponentin keskimääräinen todennäköisyys vikaantua vaateen tullessa vuoden aikana kuvaa komponentille testauksella määriteltyä vikaantumistaajuutta.

PLC *Programmable Logic Controller*. Ohjelmoitava logiikka on pieni tietokone, jota käytetään automaatioprosessien ohjauksessa. Siinä on joko modulaarisia tai integroituja tulo- ja lähtöportteja ja logiikkaosa, joka on tietokoneella ohjelmoitavissa suorittamaan haluttuja toimintoja.

SAT *Site Acceptance Testing*. Järjestelmän testaus, joka suoritetaan kun asennus lopulliseen sijoituspaikkaan on tehty. Testauksessa varmistetaan, että järjestelmä toimii oikein.

SFF *Safe Failure Fraction*. Turvallisten vikaantumisten osuus kaikista vikaantumisista. Turvalliset vikaantumiset ovat vikaantumisia, jotka laukaisevat turvatoiminnon.

SFS *Suomen Standardoimisliitto*. Suomalainen standardisoinnin keskusjärjestö, joka on kansainvälisen standardoimisjärjestön ISO ja eurooppalaisen standardoimisjärjestön CEN jäsen.

SHE *Safety, Health, Environment*. Turvallisuuteen, terveyteen ja ympäristöön liittyvät vastuuasiat.

SIF *Safety Instrumented Function*. Turva-automaatiotoiminto ohjaa prosessin turvalliseen tilaan, kun turva-automaatiojärjestelmä on tulkinnut prosessin tilan vaaralliseksi.

SIL *Safety Integrity Level*. Turvallisuuden eheyden taso määrittää yksittäisen turvatoiminnon todennäköisyyden vikaantua vaateen tullessa. Mitä suurempi prosessiriski on, sitä korkeampi turvallisuuden eheyden taso, eli turvatoiminnon toimintavarmuus vaaditaan.

SIS *Safety Instrumented System*. Turva-automaatiojärjestelmä on yksi suojauskerros, mihin kuuluu kaikki tarpeelliset laitteet ja alajärjestelmät, jotka ovat tarpeen jokaisen turva-automaatiotoiminnon suorittamiseen.

VAC *Voltage Alternating Current*. Vaihtojännite, jonka jännitevaihtelua kuvaa yleensä siniaalto.

VDC *Voltage Direct Current*. Tasajännite, jossa jännite pysyy vakiona.

1 Johdanto

Insinöörityö toteutettiin työn ohessa INEOS Composites Finland Oy:lle. Yksi tehtaalla käytetyistä riskienhallintakeinoista on relepohjainen lukitusjärjestelmä, jota ei ole sellaisenaan voitu ottaa huomioon tehtaan riskiarviossa. Tästä syystä INEOS Composites Finland Oy:llä on suunnitteilla projekti tehtaan nykyisen lukitusjärjestelmän ominaisuuksien määrittelystä; missä määrin nykyinen lukitusjärjestelmä vastaa nykyaikaisia turvajärjestelmille asetettuja vaatimuksia. Mikäli yrityksessä nähdään tutkimuksen perusteella tarpeelliseksi, suunnitelmissa on myös aloittaa hankesuunnittelu turva-automaatiojärjestelmän rakentamisesta.

Työn tavoitteena on selvittää, mitä lukitusjärjestelmällä toteutettavia turvatoimintovaatimuksia on tunnistettu prosessin riskinarvioinnissa ja mitkä niiden turvallisuuden eheyden tason vaatimukset ovat. Tämän jälkeen on tarkoitus tutustua tehtaan lukitusjärjestelmän arkkitehtuuriin ja yksittäisten turvatoimintojen toteutukseen. Tarkoituksena on saada kuva siitä, toteutuvatko riskinarvioinnissa vaaditut turvallisuuden eheyden tason vaatimukset käytännön turvatoimintojen toteutuksissa. Toinen tavoite on antaa suosituksia, kuinka tulisi edetä turva-automaatiojärjestelmän toteutuksessa, mikäli projekti päätetään aloittaa.

Työ keskittyy pääasiassa prosessiteollisuuden turva-automaatiojärjestelmän loppukäyttäjän näkökulmaan turva-automaatiojärjestelmän turvatoimintojen turvallisuuden eheyden tason vaatimuksien määrittelystä ja niiden toteutuksesta. Turva-automaatiojärjestelmään liittyvien laitteiden ja komponenttien valmistukseen, vaatimustenmukaisuuteen tai turvalogiikan ohjelmointiin liittyviin vaatimuksiin ei perehdytä tarkemmin.

Työn ensimmäisessä luvussa käydään läpi insinöörityön tausta, tavoite ja rakenne sekä esitellään insinöörityön toimeksiantaja.

Työn toisessa luvussa käydään lyhyesti läpi merkittävimmät turva-automaatiojärjestelmiä koskevat määräykset. Näihin sisältyvät direktiivit, lait, valtioneuvoston asetukset ja standardit.

Työn kolmannessa luvussa käsitellään turva-automaatiota; mitä turva-automaatiojärjestelmillä tarkoitetaan, mitä toiminnallinen turvallisuus tarkoittaa ja miksi vikaantuminen on oleellinen termi turva-automaatiojärjestelmiä käsiteltäessä.

Työn neljännessä luvussa käydään läpi turva-automaatiojärjestelmän elinkaarimalli standardin SFS-EN 61511 pohjalta. Luvussa tutustutaan erityisesti vaara- ja riskianalyysin tekoon ja turvallisuuden eheydentason varmennukseen HAZOP-tarkastelun ja LOPA-menettelyn kautta. Luvussa annetaan esimerkkejä tietyille laskennassa käytettäville arvoille, joita ei erikseen määritellä standardissa SFS-EN 61511. Yrityksen on kuitenkin itse määriteltävä nämä lukuarvot omien arvopohjiensa mukaisesti.

Työn viidennessä luvussa käsitellään INEOS Composites Finland Oy:llä käytössä olevaa turvajärjestelmää. Luvussa tarkastetaan tehtaalla tehtyä riskinarviointia, käytössä olevaa turvajärjestelmää ja sen tulevaisuutta sekä edellytyksiä liittää osaksi mahdollista tulevaa turva-automaatiojärjestelmää. Lisäksi luvussa annetaan suosituksia siitä, mitä tulisi tehdä uutta turva-automaatiojärjestelmää hankittaessa.

INEOS Composites Finland Oy

INEOS Composites Finland Oy on Porvoon Kilpilahden teollisuusalueella toimiva polyesterihartsia lujitemuoviteollisuudelle tuottava kemianteollisuuden yritys [1]. INEOS Composites Finland Oy työllistää noin 60 henkilöä. Sen liikevaihto oli vuonna 2020 noin 50 miljoonaa euroa ja tilikauden tulos oli noin 3 miljoonaa euroa [2].

INEOS Composites Finland Oy on osa INEOS Composites-liiketoimintaa. INEOS Composites-liiketoiminnalla on oma hallitus, joka vastaa toiminnastaan INEOS Group Ltd:lle. INEOS Group Ltd on kansainvälinen pörssiin

listautumaton öljy- ja kemianteollisuuden yritys, jonka pääkonttori on Lontoossa Yhdistyneessä kuningaskunnassa. INEOS Group Ltd omistaa 194 tehdasta ja konttoria 29 maasta, tuottaa vuosittain noin 61 miljardia dollaria ja työllistää 26 000 henkilöä tehden INEOS Group Ltd:stä maailman suurimman kemianteollisuuden yrityksen. INEOS Composites-liiketoiminnan lisäksi INEOS Group Ltd:llä on 35 muuta itsenäistä liiketoimintaa. [3.]

INEOS Composites-liiketoiminnan asiakkaisiin kuuluu yrityksiä rakennusteollisuudesta, kemianteollisuudesta, vene-, auto- ja asuntovaunuteollisuudesta, sekä tuulivoimateollisuudesta. INEOS Composites-liiketoiminnan valmistama polyesterihartsi on laadukasta ja asiakkaan tarpeisiin räätälöityä. Lujitemuovit ovat kestävyys-paino-suhteeltaan erinomaisia ja pitkäikäisiä eivätkä ne ruostu, lahoa tai murru kuten metalli, puu tai betoni. Ne ovat muovattavissa lähes mihin muotoon ja mittakaavaan tahansa. [4.]

Nykyisen INEOS Composites Finland Oy:n vuonna 2019 ostaman tehtaan on omistanut vuosien saatossa useat eri yritykset, mukaan lukien Neste Oy ja Ashland Finland Oy. Tehdas on rakennettu ja aloittanut tuotannon 1970-luvulla. Tehdas on vuosien mittaan laajentunut ja siellä käytetty laitekanta on tästä syystä moninaista.

2 Turva-automaatiojärjestelmiä koskevia määräyksiä

Tämän luvun tarkoituksena on käydä lyhyesti läpi turva-automaatiojärjestelmiä koskevia määräyksiä. Nämä määräykset ovat EU-direktiivejä, Suomen lakeja, Valtioneuvoston asetuksia sekä Suomen Standardisoimisliiton (SFS) standardeja.

2.1 Direktiivit, lait ja valtioneuvoston asetukset

EU-direktiivien tarkoitus on yhtenäistää EU-jäsenmaiden lainsäädännön tavoitteita siten, että maat saavat kuitenkin itse päättää laeista, joilla EU-direktiivien asettamiin tavoitteisin päästään. Turva-automaatiojärjestelmien ja toiminnallisen turvallisuuden osalta direktiivien päämääränä on saada valmistajat tuottamaan tuotteita, jotka eivät vaaranna ihmisen, koneiden tai ympäristön turvallisuutta. [5.]

Turva-automaatiojärjestelmän kannalta oleellisia direktiivejä INEOS Composites Finland Oy:ssä ovat konedirektiivi, pienjännitedirektiivi, EMC-direktiivi ATEX-laitedirektiivi ja painelaitedirektiivi. Konedirektiivi käsittelee koneiden ja niiden ohjaustoimintojen turvallisuutta koneiden valmistajan näkökulmasta [6]. Pienjännitedirektiiviä on sovellettava kaikkiin sähkölaitteisiin, joiden nimellisjännite on 50–1000 VAC tai 75–1500 VDC [7]. Direktiivi pois lukee tietyt laitteet, kuten ATEX-luokitellut laitteet. EMC-direktiivi 2014/30/EU käsittelee laitteiden sähkömagneettista yhteensopivuutta [8]. ATEX-laitedirektiivi käsittelee räjähdysvaarallisia tiloja, niissä työskentelyä sekä niissä käytettäviä sähkölaitteita ja mekaanisia turvalaitteita, säätö- ja ohjauslaitteita sekä suojausjärjestelmiä ja niihin liittyviä komponentteja, mitkä ovat ATEX-luokiteltuja [9]. Direktiivin on tarkoitus suojella räjähdysvaarallisissa työskenteleviä ihmisiä. Painelaitedirektiivi käsittelee kaikkien painelaitteiden suunnittelua ja valmistusta, joiden suunnittelupaine ylittää 0,5 bar mittaripainetta [10].

Suomen lait ovat säädöksiä, joista tärkeimmät julkaistaan ministeriöiden ja viranomaisten määräyskokoelmissa. Oikeusnormit sääntelevät oikeussubjektien

välisiä suhteita yhteiskunnassa käskien, sallien tai kieltäen jotain. Oikeusnormeilla tarkoitetaan säännön sisältävää oikeuslähdettä, kuten lain pykälää. [11.]

Työturvallisuuslain tarkoituksena on parantaa työympäristöä ja työolosuhteita työntekijöiden työkyvyn turvaamiseksi ja ylläpitämiseksi sekä ennalta ehkäistä ja torjua työtapaturmia, ammattitauteja ja muita työstä ja työympäristöstä johtuvia työntekijöiden fyysisen ja henkisen terveyden haittoja [12]. Laissa 1139/16.12.2016 varmistetaan räjähdysvaarallisissa tiloissa käytettäväksi tarkoitettujen laitteiden ja suojausjärjestelmien vaatimuksenmukaisuutta ja vapaata liikkuvuutta [13].

Valtioneuvoston asetus on Suomen lakia täsmentävä tai täydentävä säädös, joka ei muuta sitä koskevan lain sisältöä. Valtioneuvoston asetukset valmistellaan kyseisen alan ministeriössä ja ovat lakien tavoin velvoittavia. [14.]

Valtioneuvoston asetuksessa koneiden turvallisuudesta säädetään koneiden suunnitteluun ja rakentamiseen liittyvistä olennaisista terveys- ja turvallisuusvaatimuksista sekä niiden vaatimuksenmukaisuuden osoittamisesta, markkinoille saattamisesta ja käyttöönotosta [15]. Valtioneuvoston asetuksessa 685/2015 säädetään vaarallisten kemikaalien ja räjähteiden käsittelystä, varastoinnista ja säilytyksestä ja niihin liittyvistä lupa-, ilmoitus- ja hallintomenettelyistä sekä valvonnasta [16]. Valtioneuvoston asetuksessa 856/2012 säädetään vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista [17]. Valtioneuvoston asetuksen 576/2003 tarkoituksena on räjähdyskelpoisten ilmaseosten aiheuttamien vaarojen ennaltaehkäisy ja torjunta työntekijöiden turvallisuuden ja terveyden suojelemiseksi sekä yleisen turvallisuuden ylläpitämiseksi ja henkilö- ja omaisuusvahinkojen estämiseksi [18].

2.2 Standardit

Standardi on kansallisen tai kansainvälisen standardoimisjärjestön tuottama maksullinen asiakirja, joka sisältää yhteisesti sovittuja suosituksia, ohjeita tai vaatimuksia tietyistä aiheista. Näitä aiheet voivat liittyä esimerkiksi tuotteiden ominaisuuksiin, niiden valmistuksesta tai niiden testauksesta. Standardit tarkentavat direktiivien ja lainsäädäntöjen vaatimuksia. Ne voivat sisältää myös esimerkkejä siitä, kuinka niiden sisältöä tulisi toteuttaa käytännössä. Standardien noudattaminen on vapaaehtoista, mutta niitä noudattamalla voidaan osoittaa noudatettavan myös kussakin standardissa käsiteltävää asiaa koskevia direktiivejä ja lainsäädäntöä. Mikäli standardeja ei noudateta, on direktiivien ja lainsäädännön noudattaminen kyettävä osoittamaan muilla keinoin. [19.]

SFS-EN 61508

SFS-EN 61508 on toiminnallista turvallisuutta käsittelevä standardi, joka koskee sähköisistä ja/tai elektronisista komponenteista koostuvia järjestelmiä, joita käytetään turvatoimintojen suorittamiseen. Se antaa menetelmän turvallisuuteen liittyvien järjestelmien vaaditun toiminnallisen turvallisuuden saavuttamiseksi ja tarpeellisen turvallisuusvaatimusten määrittämisen kehittämiseksi. Varmentamalla laitteiden luotettavuuden standardin mukaisesti laitevalmistajat voivat vakuuttaa valmistamiensa laitteiden täyttävän niille asetetut vaatimukset. [20, s. 10.]

SFS-EN 61511

SFS-EN 61511 on standardi, joka käsittelee turva-automaatiojärjestelmän toiminnallista turvallisuutta. Se esittelee vaatimuksia turva-automaatiojärjestelmän kokonaisuudelle. [21, s. 8.]

Standardi määrittää, kuinka prosessiteollisuuden toiminnallinen turvallisuus voidaan mitoittaa prosessin tarpeisiin ihmisten, laitteiden ja ympäristön suojelemiseksi. Siinä käydään läpi vaarojen tunnistaminen riskianalyysin avulla ja riskianalyysin hyödyntäminen turvallisuusvaatimuksien mitoituksessa.

Riskianalyysin pohjalta voidaan määrittää turva-automaatiojärjestelmän turvatoimintojen turvallisuuden eheyden tason vaatimukset. Toimenpiteet ja tekniikat määritykseen esitellään standardissa, mutta turva-automaatiojärjestelmän turvatoiminnon turvallisuuden eheyden tason todentamista ei määritellä. [21, s. 46.]

SFS-EN 61511 esittää turva-automaatiojärjestelmän elinkaarimallin. Elinkaarimalli on suunnitelma, joka kattaa kaiken turva-automaatiojärjestelmän suunnittelusta, rakennuksesta ja käytöstä turva-automaatiojärjestelmän käytöstä poistoon. Elinkaarimallin tarkoitus on varmistaa turva-automaatiojärjestelmän koko elinkaaren yli jatkuvan toiminnallisen turvallisuuden hallinnan. Se sisältää tavoitteet suunnittelulle, asennukselle, käytölle, ylläpidolle ja lopulta käytöstä poistolle. [21, s. 44.]

3 Turva-automaatiojärjestelmä

Tässä luvussa tarkastetaan toiminnallista turvallisuutta ja turva-automaatiojärjestelmää, joka on osa toiminnallista turvallisuutta. Lisäksi luvussa käsitellään turva-automaatiojärjestelmien fyysistä rakennetta ja niiden vikaantumista.

Tuotannollinen liiketoiminta sisältää usein prosessista aiheutuvia riskejä. Näiden riskien tunnistaminen ja niiden siedettävälle tasolle laskeminen on työnantajan työturvallisuuslaissa asetettu lakisääteinen velvollisuus [12]. Toiminnallinen turvallisuus tarkoittaa sitä, ettei omaisuuteen tai ympäristöön kohdistuvan vahingon seurauksena syntyvän fyysisen vamman tai ihmisten terveyteen kohdistuvan vahingon sietämätöntä riskin ole olemassa [22, s. 8]. Toiminnallinen turvallisuus on yksi työturvallisuuden osa-alue, mikä sisältää kaikki turvallisuuteen liittyvät suojauskerrokset, mukaan lukien käyttö- ja turva-automaatiojärjestelmän ja on riippuvainen suojauskerrosten oikeasta toiminnasta [21, s. 20]. Yhdessä nämä laitteet muodostavat omat suojakerrokset prosessiin ja pienentävät prosessissa ilmeneviä riskejä siedettävälle tasolle [21, s. 20]. Riskiä, suojauskerroksia ja muita näihin liittyviä käsitteitä käsitellään tarkemmin luvussa 4.1.

Turva-automaatiojärjestelmän on järjestelmä, jonka tarkoitus on pienentää riskinarvioinnissa tunnistettuja riskejä, jotka jäävät rakenteellisten ratkaisujen, käyttöautomaatiojärjestelmän toimintojen ja muista suojauskerroksista syntyvien riskinalennusten jälkeen turvaamatta [21, s. 12]. Riskinarviointia käsitellään tarkemmin luvussa 4.1. Se voi olla sähköinen, elektroninen tai ohjelmoitava elektroninen järjestelmä [22, s. 14]. Käyttöautomaatiojärjestelmä on järjestelmä, joka reagoi prosessin ja operaattorin tuottamiin tulosignaaleihin ja kehittää lähtösignaaleita saaden prosessin toimimaan halutulla tavalla, mutta ei suorita mitään turvatoimintoja [21, s. 15].

Turva-automaatiojärjestelmän (Safety Instrumented System, SIS) tehtävä on saavuttaa tai säilyttää prosessin turvallinen tila käyttämällä vaadittua turvatoimintoa (Safety Instrumented Function, SIF). Turvatoiminto on turva-automaatiojärjestelmän logiikkaosan suorittama toiminto, joka perustuu tuntoelimien

antamaan tietoon prosessin tilasta ja joka vaikuttaa prosessiin toimielimien kautta halutulla tavalla. Turvatoimintoa käsitellään tarkemmin luvussa 4.4. [21, s. 29.]

3.1 Fyysinen rakenne

Automaatiojärjestelmät, kuten turva-automaatiojärjestelmät, koostuvat logiikkaosasta, tuntoelimistä ja toimielimistä. Näiden yhteen saattamisen apuna käytetään erilaisia apulaitteita, muuntimia, vahvistimia, erottimia, releitä ja muita sähkökomponentteja sekä kaapeleita ja liittimiä. Signaalimuuntimia tuloliittymissä käytetään muutettaessa analogisia viestejä digitaalisiksi ja lähtöliittimissä digitaalisia viestejä analogisiksi. [21, s. 22.]

Jokaisesta turvatoimintoon liittyvästä laitteesta on oltava luettelo, johon ne ovat selkeästi merkittyinä käyttäen laitoksen laitteistojen tunnistusmenetelmää, kuten kenttälaitetunnusten listaa. [21, s. 59.]

Logiikkaosa on joko digitaalinen ohjelmoitavissa oleva tai relepohjainen. Se toimii automaatiojärjestelmän tarkkailijana, minkä tehtävänä on suorittaa logiikkatoiminto. Logiikkatoiminto on muunnos logiikkayksikön tulotietojen ja lähtötietojen välillä tietyn ennalta määrätyn logiikan perusteella, esimerkiksi tietyssä pinnankorkeudessa venttiilin sulkeminen. [21, s. 22.] Turvalogiikan tehtävänä on siis analysoida siihen liitettyjen tuntoelimien signaaleja ja ohjata siihen liitettyjä toimielimiä suorittamalla turvatoiminnon prosessista mitattujen arvojen sitä vaatiessa.

Kenttälaitteita ovat tunto- ja toimielimet sekä käsikäyttöiset kytkimet. Kenttälaitteet ovat laitteita, jotka kykenevät suorittamaan niille määrätyn toiminnon ja jotka ovat kytketty suoraan prosessiin tai sen välittömään läheisyyteen. [21, s. 18.]

Tuntoelimien tehtävä on kerätä tietoa prosessin tilasta turvallisuuden tilan määrittämiseksi. Tuntoelimet mittaavat fyysisiä suureita, kuten lämpötilaa, painetta,

virtausta, pinnankorkeutta tai tiheyttä ja muuttavat ne sähköiseen muotoon logiikkayksikön luettavaksi.

Toimielimet toteuttavat fyysisen toiminnan ja niitä tarvitaan turvallisen tilan saavuttamiseksi tai ylläpitämiseksi [21, s. 20]. Ne saavat toimintakäskyt logiikkayksiköltä. logiikkatoimintona [21, s. 22]. Toimielimiä ovat esimerkiksi venttiilit laitteineen, moottorit ja taajuusmuuttajat. Turva-automaatiojärjestelmässä niiden tehtävänä on ohjata prosessi turvalliseen tilaan turvatoiminnon vaateen syntyessä.

Turva-automaatiojärjestelmässä käytettäviksi laitteiksi tulee valita standardin IEC 61508 mukaan sertifioituja laitteita, joista löytyy viralliset testausdokumentit eli turvallisuuskäsikirjat. Kenttälaitteita on olemassa tyyppejä A ja B. Tyypin A rakenteeltaan ja toiminnoiltaan yksinkertaisissa laitteissa kaikki vikaantumismuodot on määritelty, jolloin laitteen käyttäytyminen pystytään ennakoimaan vikatilanteen sattuessa. Tyypin B monimutkaisemmissa, usein mikropiirejä sisältävissä laitteissa kaikki vikaantumismuodot eivät ole tiedossa, eikä laitteen käyttäytymistä pystytä ennakoimaan kaikissa vikatilanteissa. [23.]

Kenttälaitteet on valittava ja asennettava niiden vikaantumisten minimoimiseksi, jotka voisivat johtaa epätarkkaan tietoon johtuen toimintaympäristöstä syntyvistä olosuhteista. Olosuhteisiin, jotka pitäisi ottaa huomioon, sisältyvät korroosio, materiaalien jäätyminen putkissa, polymerisaatio, lämpötilan ja paineen ääripäät ja kondensoituminen impulssilinjojen kuivissa haaroissa. [21, s. 69.] Laitteet on asennettava paikoilleen valmistajan ohjeita noudattaen.

3.2 Vikaantuminen

Vikaantumisella tarkoitetaan epänormaalia tilannetta, jossa turva-automaatiojärjestelmän kyky vaaditun toiminnan suorittamiselle on vähentynyt tai hävinnyt vian vuoksi. Vialla tarkoitetaan yleisesti kyvyttömyyttä vaaditun toiminnon suorittamiseen laitteen poikkeavan sisäisen tilan vuoksi. [24, s. 40.]

Turva-automaatiojärjestelmän vikaantuminen voi johtua monesta eri syystä. Vikaantumisen syy voi olla satunnaisvikaantuminen tai systemaattinen vikaantuminen [25, s. 2]. Satunnaisvikaantuminen johtuu esimerkiksi laitteen tai komponentin kulumisesta tai ikääntymisestä. Satunnaisuudestaan huolimatta satunnaisvikaantuminen noudattaa matemaattisia malleja. [25, s. 19.]

Systemaattinen vikaantuminen liittyy tiettyyn olemassa olevaan vikaan, joka tapahtuu johdonmukaisesti tietyissä olosuhteissa. Se johtuu ihmisen virheistä suunniteltaessa tai käytettäessä turvajärjestelmiä. Ne ovat siis esimerkiksi väärin määrittelyihin tai rakennus-, ohjelmointi- tai käyttövirheisiin perustuvia vikaantumisia. Systemaattista vikaantumista voidaan vähentää vain suunnittelun, valmistusprosessin, käyttömenetelmien, dokumentoinnin tai muiden merkityksellisten tekijöiden muutoksella. [21, s. 34.]

Turva-automaatiojärjestelmän vikaantuminen voi olla turvallista tai vaarallista [25, s. 3]. Turvallisessa vikaantumisessa turvatoiminnot toimivat vikaantumisen sattuessa ja siitä johtuvasta syystä halutulla tavalla [25, s. 4]. Mikäli tuvallinen vikaantuminen on paljastuvaa, turva-automaatiojärjestelmä ohjaa prosessin turvalliseen tilaan. Tällöin myös vikaantuminen tulee ilmi. Prosessin ohjaus turvalliseen tilaan voi itsessään aiheuttaa uuden vaaratilanteen. Esimerkki turvallisesta vikaantumisesta on kaapeloinnin katkeaminen kenttälaitteen ja logiikkaosan välillä lepovirtaperiaatteella toimivassa virtapiirissä.

Vaarallisessa vikaantumisessa turva-automaatiojärjestelmän turvatoiminto on estynyt reagoimasta potentiaalisesti vaaralliseen tilanteeseen [25, s. 4]. Mikäli vikaantuminen on piilevää, ei se tule prosessin normaalikäynnin aikana ilmi. Turvatoiminnon ollessa vaarallisesti piilevästi vikaantunut voi turvatoiminnon toimintavaateen syntyessä aiheutua onnettomuustilanne. Vaarallinen vikaantuminen voi johtua vääränlaisesta määrittelystä, systemaattisesta tai satunnaisesta vikaantumisesta, ohjelmointivirheestä tai esimerkiksi järjestelmän toimintaympäristön muutoksesta. Esimerkiksi työvirtaperiaatteella toimivassa virtapiirissä kaapeloinnin katkeaminen toimielimen ja logiikkaosan välillä ei tule ilmi, kunnes turvatoiminnon vaade syntyy.

Automaattisilla käytön aikaisilla diagnostiikkatesteillä on mahdollista havaita komponenttien vikaantumiset ennen turvatoiminnon vaateen syntymistä. Termillä DC_D määritetään diagnostiikan kattavuutta, joka on vaarallisten paljastuvien vikaantumisten λ_{DD} osuus vaarallisten paljastuvien λ_{DD} ja piilevien vikaantumisten λ_{DU} summasta [24, s. 54]. Laitteen tai komponentin valmistaja määrittelee vaarallisen paljastuvan vikaantumisen λ_{DD} ja vaarallisen vikaantumisen λ_D termien arvot, sekä näin ollen diagnostiikan kattavuuden.

Turva-automaatiojärjestelmät toteutetaan perinteisesti lepovirtaperiaatteella. Lepovirtaperiaate on suunnitteluperiaate, jossa releen päästäminen saa aikaan turvatoiminnon laukeamisen [26, s. 8]. Lepovirtaperiaatteella toimiva turva-automaatio tulkitsee prosessin olevan vaarallisessa tilassa esimerkiksi silloin, kun virtapiiri katkeaa. Vaihtoehto lepovirtaperiaatteelle on työvirtaperiaate. Työvirtaperiaate on suunnitteluperiaate, jossa releen veto saa aikaan turvatoiminnon laukeamisen [26, s. 8]. Käytettäessä analogiaviestejä logiikan ja kenttälaitteiden välillä on suositeltavaa pitää signaalin nollataso niin sanotusti elävänä, eli mittauksen nollatason tulisi olla suurempi kuin 0 V tai 0 mA. Tällöin kyetään havaitsemaan virtapiirin katkeaminen. Yleisesti käytetty 4–20 mA:n virtaviesti on hyvä vaihtoehto.

4 Elinkaarimalli

Turva-automaatiojärjestelmän elinkaarimallin tarkoitus on varmistaa laitosturvallisuuden riittävyys koko turva-automaatiojärjestelmän elinkaaren ajan. Turva-automaatiojärjestelmän elinkaari alkaa prosessin vaarojen ja riskien arvioinnista ja päättyy turva-automaatiojärjestelmän käytöstä poistoon. Tässä insinöörityössä käsitellään pääasiassa turva-automaatiojärjestelmän elinkaarimallin alkuosaa; turva-automaatiojärjestelmän suunnittelua ja määrittelyä.

Toiminnallisen turvallisuuden hallinta käsittelee enimmäkseen ihmisten aiheuttamia systemaattisia vikaantumisia. Toiminnallista turvallisuutta ei voida toteuttaa ilman turvajärjestelmän kanssa toimivien ihmisten osallistumista. Koko tämän henkilöstön on oltava pätevää huolehtimaan sille annetuista turvajärjestelmän elinkaaren vastuista. [28, s. 10.]

4.1 Vaaran ja riskin arviointi

Turva-automaatiojärjestelmän elinkaari alkaa prosessin vaarojen ja riskien arvioinnista. Vaara tarkoittaa tilannetta, jossa ihminen tai laitteisto joutuu vaaralliseen tilanteeseen. Vaara on siis vahingon mahdollinen lähde [21, s. 21]. Riski sisältää vaaran ja sen seurauksen, eli se määrittää vaaran suuruutta [21, s. 28].

Prosessin riski käsittää määrätyssä vaarallisessa tapahtumissa olevan riskin prosessille, käyttöautomaatiojärjestelmälle ja siihen liittyville inhimillisille tekijöille, kun riskinarvioinnissa ei ole otettu huomioon mitään turvallisuuteen liittyvää suojaustoimintoa. Se on siis raaka riski, jota suojauskerroksilla pyritään pienentämään siedettäväksi. Siedettävä riski on loppukäyttäjän määrittelemä riskin taso, joka on hyväksytty määrätyssä asiayhteydessä. Jäännösriski on riski suojauskerrosten huomioimisen jälkeen. Jos jäännösriski on pienempi kuin siedettävä riski, on riski siedettävällä tasolla. Turva-automaatiojärjestelmällä toteutetut turvatoiminnot ovat yksi prosessin suojauskerros, joilla pyritään tarvittaessa pienentämään jäännösriski siedettävän riskitason alle. [27, s. 13.]

Vaaran ja riskin arvioinnin tavoitteena on määrittää prosessin ja siihen liittyvien laitteiden vaaralliset tapahtumat, vaarallisten tapahtumaan johtavien tapahtumien järjestys, vaaralliseen tapahtumaan liittyvät prosessin riskit. Kun vaarat ovat tällä tasolla tunnistettu määritellään vaatimukset riskin pienentämiselle ja vaaditut suojauskerrokset siedettävän riskin tason saavuttamiseksi. Vaaran ja riskin arviointia varten tarvitaan tietoa prosessin suunnittelusta, miehitysjärjestelyistä ja turvallisuustavoitteista. Tässä voidaan käyttää apuna laitoksen esimerkiksi onnettomuushistoriaa, kemikaalien käyttöturvallisuustiedotteita ja raportoituja läheltä-piti-tilanteita. [21, s. 52.]

Vaaran ja riskin arviointi on suoritettava materiaaleille, prosesseille ja laitteistolle. Tuloksena on saatava aikaan kuvaus, joka sisältää jokaisen tunnetun vaarallisen tapahtuman ja siihen vaikuttavat tekijät ja vaarallisen tapahtuman todennäköisyys ja seuraukset. Kuvauksessa on otettava huomioon prosessin toimintatilojen, kuten esimerkiksi normaalin käytön, käynnistyksen, alasajon, ylläpidon, prosessin häiriötilanteen ja hätäalasajojen merkitys vaaralliseen tapahtumaan. Kuvaus sisältää myös tiedon turvatoiminnosta ja niihin liittyvästä riskin pienentämisestä. [21, s. 52.]

Jäännösriski kasvaa sen matalimmasta tasosta heti määräaikaistestauksen tai korjauksen suorittamisen jälkeen suurimpaan arvoon juuri ennen uutta määräaikaistestausta. Määräaikaistestin tarkoituksena on paljastaa turva-automaatiojärjestelmän piileviä vikoja, jotta järjestelmä voidaan korjata ”kuin uusi”-tilaan tai niin lähelle tätä, kuin käytännöllistä [21, s. 27]. Liian pitkä määräaikaistestausväli laskee turva-automaatiojärjestelmän todellista turvallisuuden eheyden tasoa, sillä turvatoiminnon satunnaisen vikaantumisen todennäköisyys kasvaa yli ajan kasvattaen turvatoiminnon suorituksen epäonnistumisten todennäköisyyttä vaateen tullessa. Jos määräaikaistestauksen välit pitkät, voi olla tarpeen määrittää suurin sallittu riskikohtainen jäännösriski, joka voidaan hyväksyä juuri ennen määräaikaistestausta. [29, s. 20.] Turvallisuuden eheyden tasoa ja turvatoiminnon todennäköisyyttä epäonnistua vaateen syntyessä käsitellään tarkemmin luvussa 4.3.

4.1.1 Suojauskerrokset

Laitoksen toiminnallinen turvallisuus on toteutettu suojauskerroksittain. Suojauskerros on mikä tahansa riippumaton mekanismi, joka pienentää riskiä ohjauksella, ehkäisemisellä tai lieventämisellä [21, s. 27].

Suojauskerroksen on oltava suunniteltu yhden mahdollisesti vaarallisen tapahtuman seurauksen suojaukseksi. Sen toiminta ei saa olla riippuvainen muista suojauskerrosten toiminnosta. Sen on oltava osoitettavasti käyttövarma ja auditoitava. Riippumattomien suojauskerrosten määrittelyä tarkennetaan luvussa 4.2.1. [27, s. 29.]

Ensimmäisessä suojauskerroksessa käyttöautomaatiojärjestelmän ja prosessihälytyksiin reagoivien operaattoreiden ohjaus- ja valvontatoimet huolehtivat laitoksen toiminnallisesta turvallisuudesta. Mikäli ohjaus- ja valvontatoimet eivät riitä estämään vaaratilanteen syntymistä, niin estotoimenpiteet toisena suojauskerroksena pyrkivät ylläpitämään toiminnallisen turvallisuuden ja ehkäisemään vaaratilanteen syntymisen. Estotoimenpiteisiin lukeutuu esimerkiksi mekaaniset suojausjärjestelmät (esimerkiksi varoventtiilit), käyttöautomaation ja operaattoreiden korjaavat toimenpiteet ja viime kädessä turva-automaatiojärjestelmä estävät riskin konkretisoitumisen. Jos vaaratilanne pääsee silti syntymään, niin kolmantena suojauskerroksena sen seuraksia pyritään lieventämään mekaanisin (esimerkiksi varoaltaat, putkien suojavaipat ja henkilökohtaiset suojaimet), turva-automaatiojärjestelmän sekä operaattoreiden avulla. [27, s. 11.]

Lieventävien kerrosten osoittautuessa riittämättömiksi on neljäntenä suojauskerroksena laitoksilla oltava harjoiteltu toimintaohje toimenpiteille hätätilanteissa. Viimeisenä suojauskerroksena suuronnettomuustilanteessa on yhdyskunnan toimenpiteet hätätilanteessa, kuten pelastuslaitosten toiminta ja hätätiedotelähetykset. Toimintaa onnettomuudessa ja suuronnettomuudessa on harjoiteltava säännöllisesti ja mahdollisesti yhdessä pelastuslaitoksen kanssa. [27, s. 11; 30.]

Prosessin vaarojen ja riskien tunnistamiseksi on suoritettava lähtötilanteen arvionti. Lähtötilanteen arvioinnin tarkoitus on kartoittaa prosessin vaaraa aiheuttaneita vaiheita. Tämän jälkeen tehdään riskikartoitus tai päivitetään olemassa oleva riskiarviointi. Lähtötilanteen arvioinnissa tulee hyödyntää aiempia riskiarvioita sekä organisaation keräämää poikkeamatietoa tapaturmista ja läheltä piti-tilanteista. Yksi lähtötilanteen arvioinnissa käytettävä riskinarviointikeino on HAZOP-tarkastelu (Hazard and Operability, HAZOP).

4.1.2 HAZOP-tarkastelu

Yksi standardissa SFS-EN 61511-3:2017 esitelty keino vaaran kvalitatiiviseen arviointiin on vaara- ja käytettävyystarkasteluanalyysi eli HAZOP-tarkastelu. Sen käyttö edellyttää yksityiskohtaista tietoa ja ymmärrystä prosessin suunnittelusta, toiminnasta ja kunnossapidosta. On epätodennäköistä, että yhdellä yksilöllä on kaikki tarvittavat tiedot ja riittävä kokemus tehdä päätöksiä kaikista asiaankuuluvista parametreista. Tästä syystä on suositeltavaa tehdä HAZOP-tarkastelu tiimityönä. Tiimin jäseniksi on suositeltavaa ottaa prosessiasiantuntija, prosessinohjausinsinööri, toimintojen hallinnan edustaja, turvallisuusasiantuntija ja henkilö, jolla on käytännön kokemusta tarkasteltavana olevan prosessin ohjauksesta. [27, s. 30.]

HAZOP-tarkastelussa kokenut tiimin johtaja ohjaa analyysitiimin järjestelmällisesti läpi prosessin suunnittelun käyttämällä soveltuvaa joukkoa parametreja ja ohjesanoja. Parametreina voidaan käyttää esimerkiksi virtausta, lämpötilaa tai painetta. Ohjesanoina voidaan käyttää sanoja kuten ei, liian vähän, liian paljon tai vasta. Näitä parametrien ja ohjesanojen yhdistelmiä, kuten esimerkiksi ”ei virtausta” tai ”vastapaine”, sovelletaan prosessin tietyissä pisteissä tai tarkasteltavissa solmukohdissa tunnistamaan mahdollisia poikkeamia tarkoitetusta toiminnasta. [27, s. 30.]

Tiimin tehtävänä on tunnistaa löydettyjen poikkeamien mahdollisia syitä sekä niiden seurauksia [27, s. 30]. Syyt voivat olla esimerkiksi ulkoisia uhkia, laitevikoja tai inhimillisiä virheitä. Ulkoisia uhkia voivat olla luonnonilmiöt, lähistöllä

tapahtuvat onnettomuudet, sabotaasi tai jopa terrorismi. Laiteviat voivat johtua ohjelmisto- tai komponenttivioista, sähkö- tai ilmakatkoista tai mekaanisten järjestelmien vioista, kuten kulumisesta, korroosiosta, värinästä, suunnittelu- tai valmistusviasta tai käytöstä suunnittelualueen ulkopuolella. Inhimillisiä virheitä ovat esimerkiksi operointivirheet ja kunnossapidon virheet. Syiden ja seurausten pohjalta pyritään määrittämään menetelmiä ja teknisiä järjestelmiä, joilla seuraukset voidaan estää tai niiden vaikutuksia vähentää. [27, s. 30.]

Jos syyt ja seuraukset ovat merkittäviä ja turvallisuustoimenpiteet riittämättömiä, tiimi voi suositella lisää turvallisuus- ja seurantatoimenpiteitä hallinnon harkittavaksi. Taulukossa 1 on esimerkki HAZOP-tarkastelun tuloksista. [27, s. 30.]

Taulukko 1. Esimerkki HAZOP-tarkastelun tuloksista [27, s. 21].

Kohde	**Parametri**	**Avainsana**	**Syyt**	**Seuraukset**	**Suojausmenetelmät**	**Toimenpide**
Säiliö	Virtaus	Suuri	Virtauksen säätöpiiri vikaantuu	Suuri virtaus johtaa suureen paineeseen		
	Paine	Suuri	1) Virtauksen säätöpiiri vikaantuu 2) Ulkoinen tulipalo	Painesäiliön vahingoittuminen ja vuoto ympäristöön	1) Suuren paineen hälytin 2) Aluelaukaisujärjestelmä 3) Paineenpoistoventtiili	Arvioidaan suunnitteluolosuhteet paineenpoistoventtiilin päästölle ympäristöön

Mikäli tuotantolaitoksella on huomattavan samanlaisia prosesseja useilla eri tuotantolinjoilla, voidaan yhden tuotantolinjan tutkinnan tuloksia käyttää pohjana seuraavien prosessien HAZOP-tarkasteluissa.

4.2 Turvatoimintojen kohdentaminen suojauskerroksille

Kun HAZOP-tarkastelu on suoritettu, prosessiin liittyvä riskin suuruus voidaan arvioida käyttämällä kvalitatiivisia tai kvantitatiivisia tekniikoita, kuten tässä insinöörityössä tarkasteltavaa semikvantitatiivista LOPA-analyysia. LOPA-analyysilla on tarkoitus kohdentaa turvatoiminnot suojauskerroksille ja määrittää jokaiselle turvatoiminnolle tarvittava turvallisuuden eheyden taso.

4.2.1 LOPA-menettely

Yksi keino tunnistetun riskin suuruuden arviointiin on suojauskerrosanalyysi eli LOPA (Layer Of Protection Analysis, LOPA). LOPA-menettelyllä analysoidaan prosessin riskien suuruutta, olemassa olevien suojauskerrosten riskinvähennysmäärää ja tarvittavien lisäsuojauskerrosten, kuten turvatoimintojen tarpeellisuutta.

Kuten HAZOP-tarkastelussa, myös LOPA-menettelyssä tarvitaan moniammatillinen tiimi. Tiimiin tulisi kuulua kokenut ja koulutettu operaattori, insinööri, jolla on asiantuntemus prosessista, valmistuksen hallinnon edustaja, prosessiohjauksen insinööri, instrumenttikunnossapidon henkilö, jolla on kokemusta tarkasteltavasta prosessista ja riskin arvioinnin asiantuntija. Jonkun edellä mainituista henkilöistä tulee olla koulutettu LOPA-metodologiaan. [27, s. 46.]

LOPA-menettelyssä tarvittavia alkutietoja ovat vaikutustapahtuma, alkusyy, suojauskerrokset ja vaadittava lievennyksen lisäys. Nämä vastaavat HAZOP-tarkastelussa kehitettyjä tietoja seuraukset, syy, olemassa olevat turvallisuustoimenpiteet ja suositellut uudet turvallisuustoimenpiteet. [27, s. 47.]

LOPA-menettelyyn tarvittavat tiedot taulukoidaan riskikohtaisesti riveittäin siten, että vaikutustapahtuman kuvaus tulee sarakkeeseen 1, vakavuustaso sarakkeeseen 2 ja niin edelleen. Jokainen erillinen suojauskerros kirjataan omaan sarakkeeseensa. Kuvassa 1 annetaan esimerkki LOPA-menettely kirjaustavasta.

#	1	2	3	4		5		6	7	8	9	10	11
					SUOJAUSKERROKSET								
	Vaikutus-tapah-tuman kuvaus F.2 F.13.2	Vaka-vuustaso F.3 F.13.2	Alkusyy F.4 F.13.3	Alkutapah-tuman taajuus vuotta kohden F.5 F.13.4	Prosessin yleinen suunnittelu F.13.5	Proses-sin käyt-tö- ja perus-automaa tio-järjes-telmä (BPCS) F.13.6	Häly-tykset ym. F.13.7	Lisänä oleva lievennys, rajoitettu pääsy, F.7 F.13.8	Riippu-mattomat suojaus-kerrokset (IPL), lisänä olevat lieventä-vät padot, paineen-päästö F.7 F.13.9	Välitapah-tuman taajuus vuotta kohden F.9 F.13.10	Turva-auto-maatio-toimin-non eheyden taso F.10 F.13.11	Lieven-netyn tapahtu-man taajuus vuotta kohden F.11 F.13.11	Huomau-tuksia
1	Tulipalo tislaus-kolonnin vaurioi-tuessa	S	Jäähdytys-veden karkaa-minen	0,1	0,1	0,1	0,1	0,1	PRV 0,01	10^{-7}	10^{-2}	10^{-9}	Suuri paine aiheuttaa kolonnin repeämise
2	Tulipalo tislaus-kolonnin vaurioi-tuessa	S	Höyryn säätöpiirin vikaan-tuminen	0,1	0,1		0,1	0,1	PRV 0,01	10^{-6}	10^{-2}	10^{-8}	Sama kuin edellä

Kuva 1. LOPA-menetelmän taulukointiesimerkki [27, s. 47].

Vaikutustapahtuman kuvauskenttään kirjataan lyhyt kuvaus riskistä, joka on tunnistettu HAZOP-tarkastelussa [27, s. 47]. Vakavuustaso-kenttään valitaan riskin vakavuustaso [27, s. 47]. Yrityksen on määriteltävä tasot itse ja määrittely on dokumentoitava. Vakavuustaso määrittää sen, kuinka suuri riski milläkin vakavuustasolla on siedettävä. Määrittely voi perustua esimerkiksi mahdolliseen henkilövahingon, ympäristövahingon tai taloudellisen tappion suuruuteen. Esimerkki vakavuustason määrittelystä annetaan taulukoissa 2, jossa vakavuustaso määritellään kategoria-sarakkeen lukuarvon perusteella.

Taulukko 2. Vakavuustason määrityksen esimerkki [31].

Kategoria	Henkilö	Ympäristö	Taloudellinen
0	Erittäin lievä loukkaantuminen	Tapahtuma, jota ei tarvitse kirjata	Kustannukset alle 100 €
1	Lievä loukkaantuminen; mutta ei menetettyä työaikaa	Kirjattava tapahtuma, mutta ei viranomaisilmoitusta tai ympäristöluvan rikkomista	Kustannukset 100 € - 1000 €
2	Yksi ei-vakava loukkaantuminen; mahdollisesti menetettyä työaikaa	Tapahtuma, joka johtaa viranomaisilmoitukseen tai ympäristöluvan rikkomiseen	Kustannukset 1000 € - 10000 €
3	Yksi tai useampi vakava loukkaantuminen	Merkittävä päästö, jolla vakavia seurauksia alueen ulkopuolella	Kustannukset 10000 € - 100000 €
4	Yksi kuolemantapaus tai pysyvä vamma	Kat. 3; lisäksi välittömiä tai pitkäaikaisia terveysvaikutuksia	Kustannukset yli 100000 €

Alkusyy-kenttään kirjataan HAZOP-tarkastelun pohjalta lyhyt kuvaus riskin alkusyystä. Alkusyitä voi olla useita ja on tärkeää luetella ne kaikki, sillä eri suojauskerrosten suojaustoiminnot saattavat koskea vain jotain tiettyä alkusyytä. Alkutapahtuman taajuus-kenttään kirjataan lähtötietojen perusteella arvio alkusyyn esiintymistodennäköisyydestä. Taajuutena käytetään tapahtumaa per vuosi. LOPA-menettelyä suorittavan tiimin kokemus on tässä erittäin tärkeää. Taulukossa 3 annetaan esimerkki alkusyyn esiintymistodennäköisyyden arviointiin. [27, s. 48.]

Taulukko 3. Esimerkki LOPA-menetelmän alkusyyn todennäköisyyden arviointiin [31].

Alkusyy	**Alkutapahtuman taajuus**
Paineastian repeäminen	10^{-6}
Putkistovuoto per 100 m putkea	10^{-3}
Tiivisteen (ei pumpun) vuoto	10^{-2}
Ulkoisen voiman vaikutus	10^{-2}
Varoventtiilin väärä aukeaminen	10^{-2}
Jäähdytysveteen liittyvä vikaantuminen	10^{-2}
Pumpun tiivisteen vuoto	10^{-1}
Käyttöautomaatiojärjestelmän säätöpiirin vikaantuminen	10^{-1}
Operaattorin virhe	10^{-1}
Pumpun vikaantuminen (muu kuin tiivistevuoto)	10^{-1}
Väärän venttiilin operointi	10^{-1}

Tapahtumataajuuden tarkan arvioinnin vuoksi on syytä hyödyntää myös laitteistosta kerättyä kunnossapitodataa taulukon 3 käytön helpottamiseksi, jotta alkusyyn tapahtumataajuus saadaan arvioitua riittävällä tarkkuudella taulukon 5 käyttöä varten.

Suojauskerrokset

Suojauskerros-osiossa kirjataan riskiin liittyvät suojauskerrokset sekä niiden riskinalennuskerroin. Riskinalennuskertoimina käytetään niille määriteltyjä suojauskerroksen toiminnon todennäköisyyttä epäonnistua vaateen sattuaessa määrittäviä PFD_{avg}-arvoja (average Probability of Failure on Demand). Suojauskerrokset, jotka eivät ole toisistaan riippumattomia, tulee huomioida laskennassa todennäköisemmin vikaantuvan toiminnon mukaan, eli suuremman PFD_{avg}-arvon mukaan. Taulukossa 4 annetaan esimerkkejä eri suojaukerrosten

PFD_{avg}-arvoista. Taulukko 4 sisältää sekä ohjaavia, ehkäiseviä että lieventäviä suojauskerroksia. Sen arvoja voidaan käyttää suuntaa antavina ohjeina myös muille suojauskerrosmenetelmille, joita ei siinä ole lueteltu. Mikäli valmistaja on ilmoittanut jollekin suojauskerrokseen kuuluvalle laitteelle PFD_{avg}-arvon, tulee valmistajan ilmoittamaa arvoa käyttää tässä yhteydessä. Turvatoimintojen PFD_{avg}-arvoja käsitellään tarkemmin luvussa 4.3.1.

Taulukko 4. Esimerkkejä erilaisille suojauskerroksille käytettävistä riskinalennuskertoimista [31].

Suojauskerroksen tyyppi	**Kuvaus / ehdot**	**PFD_{avg}-arvo**
Käyttöautomaatio-järjestelmä	Automaattinen vasteperusteinen säätöpiiri, joka on itsenäinen alkutapahtumasta	10^{-1}
Operaattorin toiminta (operointi tehtävä 10 minuutin sisällä)	Hälytysten on oltava itsenäisiä alkutapahtumasta ja muista suojauskerroksista. Operaattorin koulutuksen on sisällytettävä toiminta kyseisessä tilanteessa.	1
Operaattorin toiminta (operointi tehtävä 40 minuutin sisällä)	Hälytysten on oltava itsenäisiä alkutapahtumasta ja muista suojauskerroksista. Operaattorin koulutuksen on sisällytettävä toiminta kyseisessä tilanteessa.	10^{-1}
Passiivinen suojauskerros	Laite, jonka ei tarvitse suorittaa toimintoa vähentääkseen riskiä. Esimerkkinä suojavallit, patoaltaat yms.	10^{-2}
Vapautuslaite	Esimerkiksi varoventtiili ja murtolevy	10^{-2}
SIL 3-tason turvatoiminto	Oltava itsenäinen muista suojauskerroksista	10^{-3}
SIL 2-tason turvatoiminto	Oltava itsenäinen muista suojauskerroksista	10^{-2}
SIL 1-tason turvatoiminto	Oltava itsenäinen muista suojauskerroksista	10^{-1}

Operaattoreita varoittavien hälytysten osalta laskennassa on huomioitava operaattorin ammattitaito ja paineenalaisena toimimisen vaikutus [27, s. 49]. Hälytyksiä voivat olla esimerkiksi käyttöautomaatiojärjestelmän tai paloilmaisinlaitteiston hälytykset. Vapautuslaitteiden kategoriaan voidaan laskea lisäksi esimerkiksi sprinklerijärjestelmät.

Riippumattomat suojauskerrokset

Riippumattomat suojauskerrokset-osioon kirjataan turvatoiminnot, jotka pienentävät yksilöityä riskiä vähintään 10-kertaisesti ja ne saadaan aikaan korkealla turvallisen vikaantumisen osuuden tasolla (0,9 tai enemmän). Turvallista vikaantumista käsitellään tarkemmin luvussa 4.3.1. [27, s. 50.]

Riippumattomilla suojauskerroksilla on oltava erityisyys. Riippumaton suojauskerros on siis oltava suunniteltu estämään tai lieventämään vain yhden mahdollisen vaarallisen tapahtuman seurauksia. Samaan vaaralliseen tapahtumaan voi johtaa useampi syy, joten riippumattoman suojauskerroksen toiminnan voi käynnistää usea eri tapahtumaketju. [27, s. 50.]

Riippumattoman suojauskerroksen toiminta ei saa olla jonkin toisen suojauskerroksen onnistuneesta toiminnasta riippuvainen. Sen on oltava toimintavarma, eli sen on kyettävä tekemään se, mitä sen on suunniteltu tehtävän. Satunnaiset ja systemaattiset vikaantumismuodot on käsiteltävä suunnittelussa. [27, s. 50.]

Riippumattoman suojauksen toiminnan ylläpidon on oltava auditoitavissa. Se on määräaikaistestattava ja sen kunnossapito on varmistettava ja dokumentoitava säännöllistä kelpuutusta varten. [27, s. 50.]

Välitapahtuman todennäköisyys

Välitapahtuman todennäköisyyden sarakkeen kohdalle lasketaan alkutapahtuman taajuuden ja suojauskerroksille määritellyt PFD_{avg}-arvojen tulo [27, s. 50]. Määrittämällä riskin vakavuustaso ja välitapahtuman todennäköisyys voidaan tarkastaa, onko riski siedettävällä riskin tasolla. Määrittelyssä voidaan käyttää

taulukkoa 5. Taulukossa kuvataan riskin tasoa värein. Vihreät kentät ovat siedettävän riskin tasot. Vaalean vihreällä tasolla suojauskerrosten lisääminen ei kannata, sillä se on pienen riskin vuoksi tehotonta. Keltaisella merkityt kentät ovat tasoa, jossa voidaan tehdä toimenpiteitä suojauskerrosten lisäämiseksi, mikäli LOPA-tiimi näkee sen tarpeelliseksi. Muun väriset kentät antavat suosituksia tarvittavien toimenpiteiden nopeudesta. Kirkkaan punaisissa kentissä riski on sietämätön ja riskiä alentavat toimenpiteet suoritetaan, kun se on seuraavan kerran mahdollista. Tummanpunaisissa kentissä toimenpiteet on toteutattava välittömästi. Mustassa kentässä toiminta on lopetettava välittömästi, kunnes riski on saatu laskettua siedettävälle tasolle.

Taulukko 5. Siedettävän riskitason määrittelyn esimerkkitaulukko [31].

Taajuus/a	**Kategoria 0**	**Kategoria 1**	**Kategoria 2**	**Kategoria 3**	**Kategoria 4**
1	Siedettävän riskin taso, jota voi alentaa	Suojauskerros voidaan lisätä, mikäli tarpeellista	Suojauskerroksia lisättävä heti, kun mahdollista	Suojauskerroksia lisättävä välittömästi	Toiminta lopetettava välittömästi
10^{-1}	Suojauskerrosten lisääminen ei kannata	Siedettävän riskin taso, jota voi alentaa	Suojauskerros voidaan lisätä, mikäli tarpeellista	Suojauskerroksia lisättävä heti, kun mahdollista	Suojauskerroksia lisättävä välittömästi
10^{-2}	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Siedettävän riskin taso, jota voi alenta	Suojauskerros voidaan lisätä, mikäli tarpeellista	Suojauskerroksia lisättävä heti, kun mahdollista
10^{-3}	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Siedettävän riskin taso, jota voi alentaa	Suojauskerros voidaan lisätä, mikäli tarpeellista
10^{-4}	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Suojauskerrosten lisääminen ei kannata	Siedettävän riskin taso, jota voi alentaa

Taulukkoa 5 luetaan etsimällä ylärivistä tarkasteltavan riskin vakavuustaso. Tämän jälkeen pystysarakkeista etsitään riskin välitapahtuman todennäköisyys. Näiden kenttien risteämäkohta kertoo jäännösriskin tason. Mikäli jäännösriski ei ole siedettävällä tasolla, selataan risteävän kentän kohdalta taulukkoa alaspäin, kunnes saavutetaan siedettävän riskin taso. Saavutetulta riviltä voidaan tarkastaa riskikohtainen siedettävän riskin tason maksimitapahtumataajuus vuodessa.

Mikäli välitapahtuman todennäköisyys on suurempi kuin siedettävän riskin taso, tarvitaan lisää suojauskerroksia. Luontaisesti turvallisia menetelmiä ja ratkaisuja tulee tarkastella ennen turva-automaatiojärjestelmän turvatoimintojen valintaa. Mikäli jotain luontaisesti turvallista menetelmää kyetään hyödyntämään suojauskerroksena, on LOPA-menettelyn riskin yksilöivä rivi päivitettävä ja välitapahtuman todennäköisyys laskettava uudestaan. [27, s. 50.]

Turva-automaatiotoiminnon eheyden taso

Mikäli tarvitaan turvatoimintoa laskemaan riski siedettävälle tasolle, on määriteltävä vaadittu turvatoiminnon turvallisuuden eheyden taso. Tämä saadaan jakamalla siedettävä riskin taso välitapahtuman todennäköisyydellä. Turva-automaatiotoiminnon eheyden tason PFD_{avg}-arvon on oltava tämän jakojäännöksen alapuolella. Tämä arvo kirjataan LOPA-menettelyyn omaan kenttäänsä. [27, s. 50.]

Lievennetyn tapahtuman kenttään merkitään välitapahtuman todennäköisyyden ja turvatoiminnon eheyden tason kentän tulo. [27, s. 51.]

LOPA-menettelystä saatua dokumenttia käytetään pohjana turva-automaatiojärjestelmän turvatoimintojen suunnittelussa.

4.3 Turva-automaatiojärjestelmän turvallisuusvaatimusten erittely

Turva-automaatiojärjestelmän turvavaatimusten erittely on elinkaarimallin vaihe, jonka tarkoituksena on määritellä vaatimukset jokaiselle turvatoiminnolle ja niiden turvallisuuden eheyden tasolle, jotta saavutetaan vaadittu toiminnallinen turvallisuus. [21, s. 59.]

Turva-automaatiojärjestelmän arkkitehtuuriset vaatimukset esitetään standardissa SFS-EN 61508-2. Arkkitehtuuristen vaatimusten toteutuminen voidaan osoittaa joko kyseisessä standardissa esitettyä reittiä 1_H tai reittä 2_H pitkin. Tässä insinöörityössä tarkastetaan reittiä 1_H. Reitti 1_H perustuu laitteiston vikasietoisuuden ja turvallisten vikaantumisten osuuden konsepteihin. [32, s. 42.]

4.3.1 Turvallisuuden eheys ja turvallisuuden eheyden taso

Turva-automaatiojärjestelmän suunnittelun päätavoite on toteuttaa turvatoiminnot vastaamaan niille LOPA-menettelyssä määriteltyjä turvallisuuden eheyden tasoja. Turvallisuuden eheys määritellään turvallisuuteen liittyvän järjestelmän todennäköisyytenä suorittaa tyydyttävästi vaadittavat turvatoiminnat määritellyissä olosuhteissa määritellyllä ajanjaksona. [29, s. 22.]

Turvallisuuden eheyden taso tai SIL (Safety Integrity Level) kertoo todennäköisyyden sille, että turvallisuuteen liittyvä järjestelmä toteuttaa hyväksyttävästi vaadittavat turvatoiminnot kaikissa määritellyissä olosuhteissa ja määriteltynä ajankohtana. Turvallisuuden eheyden tasoja on neljä, joista SIL 1 on matalin ja SIL 4 on korkein. SIL 4-tasoa esiintyy perinteisesti vain hyvin korkeiden turvallisuuden eheyden tason vaatimusten laitoksissa, kuten ydinvoimaloissa.

Turvatoimintojen PFD_{avg}-arvo tarkoitta turvatoiminnon epäonnistumisen todennäköisyyttä turvatoiminnon vaateen syntyessä per vuosi. Harvojen vaateiden toimintatavan turvallisuuden eheyden tasojen PFD_{avg}-vaatimukset on esitetty taulukossa 6.

Vaateisissa toimintatavoissa turvatoiminnon vaarallinen vikaantuminen voi aiheuttaa vaarallisen tapahtuman, mikäli vikaantumista ei havaita ja vaade esiintyy ennen seuraavaa määräaikaistestiä. Myös havaittu vikaantuminen voi aiheuttaa vaarallisen tapahtuman synnyn, mikäli prosessia ja siihen liittyviä laitteita ei ole siirretty turvalliseen tilaan ennen vaateen esiintymistä. [21, s. 24.]

Harvojen vaateiden toimintatavassa turva- ja käyttöautomaatio on eriytetty, eli muut järjestelmät eivät vaaranna turvatoiminnon suoritusta. Turvatoiminto suoritetaan harvojen vaateiden toimintatavassa vain vaateesta ja vaade turvatoiminnolle tulee harvemmin kuin kerran vuodessa. Tässä insinöörityössä käsitellään pääasiassa harvojen vaateiden toimintatapaa. [21, s. 23.]

Taulukko 6. Harvojen vaateiden SIL-luokitukset ja niitä vastaavat PFD_{avg}-arvot [21, s. 54]. Muuttuja f [1/a] kuvaa turvatoiminnon PFDavg-arvoa.

SIL-taso	**PFD_{avg}**
SIL 4	$10^{-5} \geq f < 10^{-4}$
SIL 3	$10^{-4} \geq f < 10^{-3}$
SIL 2	$10^{-3} \geq f < 10^{-2}$
SIL 1	$10^{-2} \geq f < 10^{-1}$

PFD_{avg}-arvo lasketaan perinteistesti määrittämällä kullekin turvatoiminnon osatekijälle PFDavg-arvo, jonka valmistaja on ilmoittanut. Näitä osatekijöitä ovat tuntoelimet apulaitteineen, logiikkayksikkö IO-moduuleineen ja toimielimet apulaitteineen. Osatekijöiden PFD_{avg}-arvot lasketaan yhteen, jolloin laskennan summa on turvatoiminnon PFD_{avg}-arvo. Laskennassa käytettävä kaava riippuu turvatoiminnon äänestysrakenteesta. Äänestysrakennetta käsitellään tarkemmin seuraavassa luvussa. [33.]

Tiheiden tai jatkuvien vaateiden toimintatavassa vaade turvatoiminnolle esiintyy useammin kuin kerran vuodessa tai jatkuvasti ja turvatoiminto suoritetaan vain vaateesta [21, s. 24]. Jatkuvassa toimintatavassa turvatoiminto pitää prosessin turvallisessa tilassa osana normaalia toimintaa, eli käytännössä ohjaa prosessia yhdessä käyttöautomaatiojärjestelmän kanssa. Turvatoiminnon onnistumisen todennäköisyyttä turvatoiminnon vaateen syntyessä mitataan käsitteellä PFH_d (Probability of dangerous Failure per Hour). PFH_d-arvo ilmoittaa, kuinka monta kertaa per tunti turvatoiminto epäonnistuu [21, s. 55]. Tämä insinöörityö ei käsittele tiheiden tai jatkuvien vaateiden toimintatapojen turvatoimintoja, vaan keskittyy harvojen vaateiden toimintatapojen turvatoimintoihin.

4.3.2 Äänestysrakenne ja vikasietoisuus

Myös turva-automaatiojärjestelmän arkkitehtuuri ja käytettävien laitteiden turvallisten vikaantumisten osuus (Safe Failure Fraction, SFF) asettaa tietyt

minimivaatimukset sille, mitä turvallisuuden eheyden tasoa voidaan käyttää. Turvallisen vikaantumisen osuuden rajoitukset esitetään taulukossa 7. A- ja B-tyypin laitteille vikasietoisuuden perusteella sallittavat SIL-tasot ovat erilaisia ja ne riippuvat turvallisten vikaantumisten osuudesta.

Taulukko 7. Turva-automaatiojärjestelmään kuuluvan laitteen tai komponentin turvallisten vikaantumisten osuuden vaikutus sallittuun turvallisuuden eheyden tasoon [32, s. 46 ja 48].

Elementin turvallisten vikaantumisten osuus	**Elementin tyyppi**	**Laitteiston vikasietoisuus**		
		0	**1**	**2**
< 60 %	A	SIL 1	SIL 2	SIL 3
	B	Ei sallittu	SIL 1	SIL 2
60 % - < 90 %	A	SIL 2	SIL 3	SIL 4
	B	SIL 1	SIL 2	SIL 3
90 % - < 99 %	A	SIL 3	SIL 4	SIL 4
	B	SIL 2	SIL 3	SIL 4
≥ 99 %	A	SIL 3	SIL 4	SIL 4
	B	SIL 3	SIL 4	SIL 4

Laitteen turvallisten vikaantumisten osuus lasketaan kaavalla 1 [32, s. 130].

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \quad (1)$$

λ_S on turvallinen vikaantuminen

λ_{DD} on vaarallinen paljastuva vikaantuminen

λ_D on vaarallinen vikaantuminen, jossa λ_D on λ_{DD}:n ja λ_{DU}:n summa.

Laitteen valmistaja ilmoittaa kaavassa 2 esitettyjen termien arvot. Tietyssä turvapiirissä käytettyjen komponenttien on yllettävä turvallisen vikaantumisen osuudeltaan turvapiirin turvallisuuden eheyden tason asettamalle vaatimustasolle.

Turvatoiminnon vikasietoisuuden parantamiseksi ja tarpeettomien turvatoimintojen laukaisujen estämiseksi voidaan käyttää erilaisia turvatoimintojen laukaisujen äänestysrakenteita. Vikasietoisuudella tarkoitetaan toiminnallisen yksikön kykyä jatkaa vaaditun toiminnon suorittamista vikojen tai virheiden ollessa läsnä [21, s. 20].

Äänestysrakenteet merkitään muodossa MooN (M out of N) [21, s. 24]. N kertoo turvatoimintoon liittyvien riippumattomien kanavien määrän. Laitetta tai laiteryhmää, joka riippumattomasti suorittaa määrätyn turvatoiminnon kutsutaan turvaautomaatiojärjestelmän kanavaksi. Kanavan laitteisiin voi sisältyä tulo- ja lähtölaitteita sekä logiikkaosa. Monikanavakonfiguraatiossa useampi kanava suorittaa riippumattomasti samaa toimintoa. Nämä kanavat voivat olla identtisiä tai erilaisia. [21, s. 15.]

MooN-äänestysrakenteessa M kertoo, kuinka monen kanavan on vaadittava turvatoiminnon laukaisua, jotta turvatoiminnon laukaisu tapahtuu. 1oo1-äänestysrakenteessa on siis yksi kanava, kun kaksoiskanavakonfiguroidussa 1oo2-äänestysrakenteessa niitä on kaksi. Laitteiston vikasietoisuus (Hardware Fault Tolerance, HFT) X tarkoittaa, että X+1 yhtäaikaista vikaa voi johtaa turvatoiminnon menettämiseen. Vikasietoisuus saadaan laskemalla äänestysrakenteesta MooN N - M = X. [34.]

1oo1-äänestysrakenne on kaikista yksinkertaisin rakenne. Siinä ei ole redundanssia ja se on sekä turvallisuus- että luotettavuusmielessä heikko. Turvallinen vikaantuminen aiheuttaa tässä äänestysrakenteessa välittömästi turvatoiminnon laukeamisen. Vaarallinen vikaantuminen aiheuttaa turvatoiminnon vikaantumisen. Äänestysrakenteena se on kaikista edullisin. Kaavassa 2 esitetään 1oo1-äänestysrakenteen PFD_{avg}(1oo1) -arvon laskentakaava. [34.]

$$PFD_{avg}(1oo1) = (\lambda_{DD} + \lambda_{DU}) * t_{CE} \quad (2)$$

λ_{DU} on varallinen piilevä vikaantuminen.

Laitteen valmistaja määrittelee kaavassa 2 käytetyn vaarallisen piilevän vikaantumisen termin λ_{DU} arvon. Termi t_{CE}(1oo1) määrittää kanavakohtaisen

vikaantuneenaoloajan. Kaavassa 2 esiintyvän termin $t_{CE}(1oo1)$ laskentakaava esitetään kaavassa 3. [35.]

$$t_{CE}(1oo1) = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (3)$$

T_1 on määräaikaiskoeistusväli [h]
MTTR (Mean Time To Restore) on ennalta määritelty palautumisaika [h].

Laitteiston käyttäjä määrittelee itse käytettävän määräaikaiskoestusvälin T_1 ja arvioi vikaantuneen laitteen palautumisajan MTTR. Vikaantuneen laitteen palautumisaika kattaa ajan vikaantumisen havaitsemisesta sen korjaukseen ja käyttöönottoon. Vikaantuneen laitteen korjausajassa on huomioitava muun muassa varaosien saatavuus, työlupakäytännöt ja kunnossapito-organisaation tai ulkoisten palveluntarjoajien työ- ja päivystysajat. [24, s. 48.]

1oo2-äänestysrakenteessa on kaksi itsenäistä kanavaa. Turvatoiminto laukeaa, mikäli toinen kanavista sitä vaatii. Tästä syystä 1oo2 on luotettavuusmielessä huonompi äänestysrakenne kuin 1oo1, sillä siinä on kaksi potentiaalisesti vikaantuvaa kanavaa yhden sijaan. Turvallisuusmielessä se taas on parempi ratkaisu. Systemaattisen vikaantumisen välttämiseksi eri kanavien laitteiden tulisi olla keskenään erilaisia, esimerkiksi erityyppisiä, eri tekniikkaa hyödyntäviä, eri virtalähteiden syöttämiä tai eri valmistajan valmistamia. Hinnaltaan 1oo2-äänestysrakenne on laitteistosta riippuen kalliimpi kuin 1oo1-äänestysrakenne. Kaavassa 4 esitetään 1oo2-äänestysrakenteen $PFD_{avg}(1oo2)$ -arvon laskentakaava. [34.]

$$PFD_{avg}(1oo2) = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \quad (4)$$

β_D on vaarallisten paljastuvien yhteisvikaantumisten osuus.
β on vaarallisten piilevien yhteisvikaantumisten osuus.

Beeta-termit β_D ja β määrittävät varallisten yhteisvikaantumisten osuudet. Ne ovat niin sanottuja virtuaaliblokkeja, jotka ovat laskennallisesti sarjassa kanava- ja äänestyspiirikohtaisten vikaantumisten kanssa. Laitteen käyttäjä määrittelee

kaavassa esiintyvien termien β_D ja β arvot. Termin β_D arvo voi olla joko 10 % tai 20 %. Termin suuruus riippuu siitä, kuinka keskenään erilaisia kanavat ovat. Termin β arvo on kaksinkertainen termin β_D arvoon nähden. Joissain tapauksissa valmistaja voi määritellä termien β_D ja β arvoiksi 1 % ja 2 %. Tällöin valmistajan ilmoittamia arvoja on käytettävä. [35.]

Termi $t_{GE}(1oo2)$ määrittää äänestysporttikohtaisen vikaantuneenaoloajan. Äänestysporttikohtainen vikaantuminen syntyy silloin, kun turvatoiminto ei enää toimi riittävän monen kanavan vikaantuessa. 1oo2-äänestysrakenteessa tarvitaan siis molempien kanavien yhtäaikainen vaarallinen piilevä vikaantuminen. Kaavassa 5 esiintyvän termin $t_{GE}(1oo2)$ laskentakaava esitetään kaavassa 5. [34.]

$$t_{GE}(1oo2) = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (5)$$

2oo2-äänestysrakenteessa on kaksi itsenäistä kanavaa. Laskennaltaan se on 1oo1-äänestysrakennetta vastaava. Rakenteeltaan se vastaa 1oo2-äänestysrakennetta. Turvatoiminto laukeaa, mikäli molemmat kanavat sitä vaativat. Kaavassa 6 esitetään 1oo2-äänestysrakenteen $PFD_{avg}(2oo2)$ -arvon laskentakaava. Luotettavuusmielessä 2oo2-äänestysrakenne on hyvä valinta, sillä tarpeettomia turvatoiminnon laukaisuja ei todennäköisesti synny usein. Turvallisuusmielessä rakenne on heikompi, sillä kumman tahansa kanavan vaarallinen piilevä vikaantuminen estää turvatoiminnon laukeamisen. [34.]

$$PFD_{avg}(2oo2) = 2 * (\lambda_{DD} + \lambda_{DU}) * t_{CE} \quad (6)$$

1oo3-äänestysrakenteessa on kolme itsenäistä kanavaa. Turvatoiminto laukeaa, mikäli yksi kolmesta kanavasta sitä vaatii. Tässä äänestysrakenteessa kahden kanavan vaarallinen piilevä vikaantuminen ei estä turvatoiminnon oikeaa toimintaa, eli turvatoiminnon vikasietoisuus on 2. 1oo3-äänestysrakenteen turvallisuus on erittäin hyvä, mutta luotettavuus heikko. Yhdenkin kanavan turvallinen vikaantuminen aiheuttaa turvatoiminnon laukaisun. Sen hinta on myös

laitteistosta riippuen kallein. Kaavassa 7 esitetään 1oo3-äänestysrakenteen PFD_{avg}(1oo3) -arvon laskentakaava [34].

$$PFD_{avg}(1oo3) = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU}(\frac{T_1}{2} + MTTR) \quad (7)$$

Kaavassa 8 esiintyvän termin t_{GE}(1oo3) laskentakaava esitetään kaavassa 8 [34].

$$t_{GE}(1oo3) = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (8)$$

Kaavassa 7 esiintyvän termin t_{G2E} kaava vastaa termiä t_{GE}(2oo3).

2oo3-äänestysrakenteessa on kolme itsenäistä kanavaa. Turvatoiminto laukeaa, mikäli kaksi kolmesta kanavasta sitä vaatii. Tässä äänestysrakenteessa yhden kanavan vaarallinen piilevä vikaantuminen ei estä turvatoiminnon oikeaa toimintaa, eli turvatoiminnon vikasietoisuus on 1. Yhden kanavan turvallinen vikaantuminen ei myöskään laukaise turvatoimintoa, mikäli muut kanavat toimivat oikein. 2oo3-äänestysrakenteen luotettavuus ja turvallisuus ovat näistä vaihtoehdoista parhaat. Kaavassa 9 esitetään 2oo3-äänestysrakenteen PFD_{avg}(2oo3) -arvon laskentakaava [34].

$$PFD_{avg}(2oo3) = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta_D \lambda_{DU}(\frac{T_1}{2} + MTTR) \quad (9)$$

Kaavassa 9 esiintyvän termin t_{GE}(2oo3) laskentakaava esitetään kaavassa 10 [35].

$$t_{GE}(2oo3) = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (10)$$

Turvatoiminnon sopiva äänestysrakenne on valittava turva-automaatiojärjestelmän toimintatavan, laitetyypin ja turvatoiminnon turvallisuuden eheyden tason

vaatimuksen perusteella. Valinnassa on syytä tarkastella vähimmäisvaatimusta äänestysrakenteelle, äänestysrakenteiden kustannuksia ja niiden vaatimaa ylläpitoa ja vaikutusta määräaikaistestausten mittakaavaan.

4.3.3 Systemaattinen kyvykkyys

Systemaattinen kyvykkyys koskee laitevalmistajien vaatimuksia. Standardi IEC 61508 määrittelee systemaattisen kyvykkyyden luottamuksen mittana siitä, että laitteen systemaattinen eheys täyttää määritellyn turvallisuuden eheyden tason vaatimuksen määritellyn laitteen turvatoiminnon suhteen. Laitetta on käytettävä valmistajan vaatimusten mukaisesti. Systemaattinen turvallisuus on siis loppukäyttäjän toimesta yksinkertaista osoittaa käyttämällä IEC 61508 sertifioituja laitteita. [36.]

IEC 61508 asettaa valmistajalle vaatimuksia ohjelmajärjestyksen valvonnasta, on-line-viantunnistuksesta, testeistä redundanttilaitteistolla, prosessorien testauksista, koodisuojista ja laitteiston monipuolisuudesta. Nämä tekijät määrittelevät vaatimusten perusteella sen, millaisen SIL-luokituksen laitteelle voidaan myöntää. Kunkin tekniikan tai toimenpiteen osalta ilmoitetaan, onko se pakollinen, erittäin suositeltava, suositeltava tai ei suositeltava. IEC 61508 sertifioidut laitteet ovat akkreditoidun kolmannen osapuolen suorittaman auditoinnin läpäisseitä. [36.]

4.4 Turva-automaatiojärjestelmän suunnittelu

Turva-automaatiojärjestelmän suorittaman turvatoiminnon tarkoitus on saavuttaa tai pitää prosessille turvallinen tila tiettyyn vaaralliseen tapahtumaan nähden ja näin alentaa tunnistettu prosessin riski siedettävälle tasolle [21, 29]. Turvatoiminnosta vastaava turvapiiri sisältää joukon kyseiseen turvatoimintoon soveltuvia tunto- ja toimielimiä, kaapeleita, liittimiä ja apulaitteita.

Turvatoiminnon lauettua toimielimien palautuminen normaalitilaan on tapahduttava vasta, kun suojausehdot ovat normaalitilassa ja nollaus on käynnistetty,

ellei muutoin ole määritelty turvallisuusvaatimusten erittelyssä [21, s. 62]. Turvatoiminnot voidaan tarpeen mukaan ohittaa, eli estää turvatoiminnon toiminnallisuuden suorittaminen kokonaan tai osittain [21, s. 15]. Ohitus voidaan suorittaa esimerkiksi huolto-ohituskytkimillä. Huolto-ohituskytkimien tulee olla suojattuna valtuuttamattoman käytön estämiseksi [21, s. 70].

Kaikista turvatoiminnoista on oltava kuvaus, joka voi olla esimerkiksi turvatoiminnon logiikan sanallinen selostus tai syy- ja seurauskaavio. Kuvaukseen on sisällytettävä tiedot turva-automaatiojärjestelmän prosessimittauksista ja niiden mittausalueista, mittatarkkuuksista ja laukaisurajoista. Kuvauksen on oltava selkeä, tarkka, todennettava, ylläpidettävä ja toteuttamiskelpoinen. Jokainen liityntä turva-automaatiojärjestelmän ja muiden järjestelmien välillä on määriteltävä. Muita järjestelmiä voivat olla esimerkiksi käyttöautomaatiojärjestelmä ja operaattorit. Turva-automaatiojärjestelmän riippumattomuus muista järjestelmistä on säilytettävä ja kyettävä osoittamaan. [21, s. 59.]

Jokaiselle turvatoiminnolle on oltava myös määriteltynä prosessin turvallinen tila. Turvallisessa tilassa on prosessissa saavutettu vakaa tila ja määritelty vaarallinen tapahtuma on vältetty tai sitä on lievennetty riittävästi. Jotkin itsessään turvalliset prosessin tilat voivat yhdessä esiintyessään aiheuttaa vaaran, ja myös nämä on määriteltävä. [21, s. 59.]

Äärimmäiset ympäristöolosuhteiden arvot tulee arvioida ja ottaa huomioon turva-automaatiojärjestelmää suunniteltaessa. Ympäristöolosuhteisiin kuuluvat muun muassa lämpötila, kosteus, epäpuhtaudet, maadoitus, sähkömagneettinen ja muu säteily, iskut ja tärinä, staattinen sähkö, sähköteknisien alueiden luokitukset, tulviminen ja salamointi. [21, s. 60.]

Jokaiselle turvatoiminnolle on oltava määriteltynä turvatoiminnon nollausmenetelmä alasajon jälkeen. Nollausmenetelmä vapauttaa turva-automaatiojärjestelmän pakko-ohjaamat turvatoiminnot takaisin normaalitilaan, jolloin prosessi voi jatkaa toimintaansa. Nollausmenetelmät voivat olla manuaalisia, puoliautomaattisia tai automaattisia. Nollaus voi tapahtua esimerkiksi kytkimellä tai turva-

automaatiopiirin tuntoelimen mittauksen palauduttua turvalliselle tasolle. Turvatoimintojen ohituksille on oltava kirjalliset menettelytapaohjeet, jotta ohitukset hallitaan ja myöhemmin poistetaan. [21, s. 60.]

Turvatoiminnon on oltava riittävän nopea. Jokaiselle turvatoiminnolle on asetettava vasteaikavaatimus, jotta prosessi voidaan ohjata turvalliseen tilaan prosessin turva-ajan sisällä [21, s. 59]. Prosessin turva-ajalla tarkoitetaan aikaa, joka kuluu prosessin, käyttö- tai turva-automaatiojärjestelmän vikaantumisesta vaaralliseen tapahtumaan, kun turvatoimintoa ei vikaantumisesta johtuen suoriteta [37, s. 58].

Turva-automaatiojärjestelmän toimintatapavaade tulee määritellä. Kullekin turvatoiminnolle on määriteltävä myös oletettu vaadetaajuus. [21, s. 59.]

Turva-automaatiojärjestelmää suunniteltaessa tulisi ottaa huomioon myös prosessin normaalit ja epänormaalit toiminta- ja käyntitilat, kuten prosessin käynnistys, normaali käynti ja (hallittu) alasajo. Eri prosessivaiheet voivat olla olosuhteiltaan hyvin erilaisia. Turva-automaatiojärjestelmän ei tulisi estää prosessin normaalia toimintaa ennakoitavissa olevissa toiminta- ja käyntitiloissa. [21, s. 60.]

Turva-automaatiojärjestelmän ylläpidon kannata kriittisen tilatiedon on oltava saatavana osana käyttöliittymää. Tähän tietoon voi sisältyä tiedot turva-automaatiojärjestelmän turvatoiminnon tiloista, kuten tunto- ja toimielimien tilatiedoista, turvatoiminnon laukeamisesta, ohituksesta tai äänestyksen vajaatoiminnasta sekä diagnostiikan tuloksista, kuten vikatiloista tai energian menetyksestä. Lisäksi on saatava tieto ympäristöolosuhteita ylläpitävien laitteiden vikaantumisesta, mikäli ne ovat turva-automaatiojärjestelmän toiminnan kannalta merkityksellisiä. [21, s. 70.]

4.4.1 Turva-automaatiojärjestelmän erillisyys

Jos käyttöautomaatiojärjestelmää ei ole tarkoitus kelpoistaa standardin IEC 61511 mukaisesti, niin turva-automaatiojärjestelmä on suunniteltava käyttöautomaatiojärjestelmästä erilliseksi ja riippumattomaksi siinä laajuudessa, ettei turva-automaatiojärjestelmän turvallisuuden eheys vaarannu. [21, s. 62.]

Turva-automaatio voi välittää tilatietoja käyttöautomaatiojärjestelmään, mutta ei toisin päin. Turva-automaatiojärjestelmän turvatoimintoja kutsutaan prosessiteollisuudessa usein lukituksiksi, jotka ovat korkeamman prioriteetin ohjauksia muihin prosessia ohjaaviin järjestelmiin nähden. Turva-automaatiojärjestelmän turvatoiminnot siis yliajavat esimerkiksi käyttöautomaatiojärjestelmän ohjaukset, mikäli molemmat yrittävät ohjata samaa toimilaitetta. [38.]

Turva-automaatiojärjestelmän eriyttämisen käyttöautomaatiojärjestelmästä etuja ovat yhteismuotoisten ja systemaattisten virhelähteiden minimointi, käyttöautomaation kevyempi muutoksenhallinta (turva-automaatiojärjestelmän elinkaarimalli), turva-automaatiojärjestelmän selkeä identifiointi käyttöautomaatiosta ja parempi tietoturva ja kyberturvallisuus. Eriyttämisen haittoja ovat korkeammat suunnittelu-, testaus-, huolto- ja asennuskulut, suurempi varaosamäärä, turva- ja käyttöautomaation rajapinnan määrittely- ja dokumentointitarve, erilaiset suunnittelutyökalut, hälytyskäytännöt ja raportoinnit ja suurempi koulutustarve käytettävyyttä ajatellen. [38.]

Turva-automaatiojärjestelmän sovellus sisältää myös muita vaatimuksia käyttöautomaatiojärjestelmästä erillisyyden lisäksi, mutta turva-automaatiojärjestelmän sovellusvaatimukset eivät kuulu tämän insinöörityön piiriin. [38.]

4.5 Muut elinkaarimallin tasot

Tässä osiossa käydään lyhyesti läpi loput turva-automaatiojärjestelmän elinkaarimallin tasot. Tämä insinöörityö keskittyy turva-automaatiojärjestelmän suunnittelun vaatimuksiin, ja elinkaarimallin muut tasot käydään läpi siltä osin, kuin se

on oleellista insinöörityön tilaajan kannalta. Tarkemmat ohjeistukset turva-automaatiojärjestelmän elinkaarimallin käytännön toteuttamiseen löytyvät standardista SFS-EN 61511-2:2017.

4.5.1 Turva-automaatiojärjestelmän asennus, käyttöönotto ja kelpuutus

Turva-automaation elinkaarimallin asennuksen, käyttöönoton ja kelpuutuksen osan tarkoituksena on kelpuuttaa turva-automaatiojärjestelmän turvallisuusvaatimukset turvatoimintojen ja turvallisuuden eheyden tason osalta. Lisäksi sen tarkoituksena on testata turva-automaatiojärjestelmä ja integroida se käyttöön. Asennusta, käyttöönottoa ja kelpuutusta kutsutaan myös laitoshyväksyntätestiksi (Site Acceptance Testing, SAT). [37, s. 118.]

Kun tämä elinkaarimallin vaihe on suoritettu, voidaan todeta, että turva-automaatiojärjestelmä on täysin toimiva ja turva-automaatiojärjestelmän turvallisuusvaatimusten mukainen. Tuloksena on dokumentaatio integrointitesteistä, asennus-, käyttöönotto- ja kelpuutustoiminnoista. [37, s. 118.]

Asennuksen, käyttöönoton ja kelpuutuksen hoitaa perinteisesti rakentaja yhteistyössä suunnittelu- ja asennusryhmän sekä laitteiston käyttäjän kanssa. [37, s. 118.]

4.5.2 Turva-automaatiojärjestelmän käyttö, ylläpito ja muutokset

Turva-automaatiojärjestelmän elinkaarimallin käyttö- ja ylläpitovaiheen tärkein tehtävä on varmistaa, että turva-automaatiojärjestelmän toiminnallinen turvallisuus ylläpidetään käytön ja ylläpidon aikana. Käyttö- ja ylläpitotoiminnot dokumentoidaan. [37, s. 118.]

Tarvittaessa turva-automaatiojärjestelmään tehdään korjauksia tai parannuksia. Näitä toimenpiteitä käsitellään elinkaarimallin muutosten osassa. Muutoksia tehtäessä on varmistettava, että vaadittu turvallisuuden eheyden taso saavutetaan tai ylläpidetään. Myös nämä toimenpiteet dokumentoidaan. Etenkin suuria

muutoksia toteutettaessa on palattava elinkaarimallin suunnitteluvaiheeseen. Myös merkittävät muutokset prosessiin ja sen turvallisuuteen voi vaatia turva-automaatiojärjestelmän osalta palaamista elinkaarimallin vaaran ja riskin arviointivaiheeseen. [37, s. 119.]

4.5.3 Käytöstä poisto

Turva-automaatiojärjestelmän elinkaarimallin käytöstä poiston vaiheen tarkoituksena on varmistaa sopiva katselmointi käytöstä poistoon ja varmistaa, että turvatoiminnot pysyvät asianmukaisina. Tärkeintä on ylläpitää prosessin turvallisuustaso ihmisille, liiketoiminnalle ja ympäristölle riittävänä. [37, s. 118.]

5 INEOS Composites Finland Oy:n turvajärjestelmä

Tässä luvussa tarkastetaan turvajärjestelmän toteutusta INEOS Composites Finland Oy:ssä. Yrityksellä on suunnitelmissa uusia turvajärjestelmä turva-automaatiojärjestelmäksi, joka vastaa sille nykyisin asetettuja vaatimuksia. Insinöörityön tarkoituksena oli selvittää nykyisin käytössä olevan turvajärjestelmän soveltuvuus tulevan turva-automaatiojärjestelmän asettamiin vaatimuksiin. Tarkoituksena oli selvittää, missä määrin nykyinen turvajärjestelmä voidaan säilyttää osana tulevaa turva-automaatiojärjestelmää. Insinöörityön tarkoituksena oli tarkastella laitoksesta tehtyä riskinarviointia, selvittää käytössä olevan turvajärjestelmän edellytykset saavuttaa vaadittua turvallisuuden eheyden tasoja riskinarvioinnissa tunnistettujen turvatoimintojen vaateiden osalta ja antaa suosituksia, kuinka vaaditut riskinarvioinnissa tunnistetut turvatoiminnot tulisi toteuttaa turva-automaatiojärjestelmässä.

5.1 Selvityksen suorituksen kuvaus

INEOS Composites Finland Oy:llä käytössä olevan turvajärjestelmän tilan selvitystyö aloitettiin tarkastelemalla laitoksesta tehtyä riskinarviointia. Riskinarviointia käsitellään tarkemmin seuraavassa luvussa. Riskinarviointi on hyvin laaja, eikä insinöörityöhön käytössä olevalla ajalla olisi kyetty käymään koko arviota seikkaperäisesti läpi. Tästä syystä johtuen riskinarvioinnin tarkastelussa keskityttiin pääasiassa niihin tunnistettuihin riskeihin, joiden jäännösriski ennen turva-automaatiotoimintojen huomioimista oli sietämättömällä tasolla. Näiden riskien osalta tarkastettiin mitä turvallisuuden eheyden tason vaatimusta ne edellyttivät jäännösriskin siedettävälle tasolle saamiseksi. Tarkastelussa huomattiin, että riskit kohdistuivat pääasiassa hyvin samankaltaisiin prosessin vaaroihin.

Seuraava vaihe oli tarkastella näiden riskien osalta olemassa olevien turvatoimintojen piirikaavioita, kojeluetteloita sekä putkisto- ja instrumentointikaavioita. Lisäksi tarkasteltiin turvajärjestelmästä ja prosessista olemassa olevaa dokumentaatiota, kuten prosessikuvauksia. Tarkastelussa kävi nopeasti ilmi, että mikäli insinöörityön tavoitteena olisi käydä läpi kaikki riskinarvioinnissa

turvatoimintoja vaativat riskit, eli turvajärjestelmässä olemassa olevat turvapiirit, kävisi läpi käytävän dokumentaation määrä insinöörityön ajankäytön näkökulmasta liian suureksi.

Tästä syystä tarkastelussa keskityttiin ensin pelkästään piirikaavioiden ja kojeluetteloiden läpikäyntiin. Näitä tarkasteltaessa kävi ilmi, että turvapiirit ovat keskenään hyvin samankaltaisia. Osa turvapiireistä liittyy yhden prosessilaitteen turvaamiseen, osa useamman. Logiikkaosa oli käytännössä kaikilla käytössä olevilla turvapiireillä samanlainen. Logiikkaosaa käsitellään tarkemmin luvussa 5.3.1. Käytettävät kenttälaitteet ovat melko samankaltaisia laitoksen käyttöautomaatiojärjestelmässä käytettävien laitteiden kanssa, eikä merkittäviä eroja automaatiojärjestelmästä riippumatta löytynyt. Kenttälaitteita käsitellään tarkemmin luvussa 5.3.2. Näistä syistä johtuen etsittiin yleisesti turvajärjestelmää kattavasti edustava turvapiiri, joka turvasi useita prosessilaitteita, käytti muissakin turvatoiminnoissa käytettäviä tunto- ja toimielimiä sekä signaalin käsittelyyn liittyviä apulaitteita ja kuittauskytkimiä. Valittua turvapiiriä käsitellään tarkemmin luvussa 5.3.3.

Esimerkkipiirin käyttäminen yleistyksenä koko lukitusjärjestelmästä on käyttökelpoinen antamaan kuvan turva-automaatiojärjestelmän suunnittelu- ja hankintaprosessin laajuudesta ja vaatimuksista liittyen elinkaarimallin mukaisiin toimenpidevaatimuksiin. Näitä vaatimuksia käsitellään tarkemmin luvussa 5.4. Pelkistykseen liittyy myös haasteita. Insinöörityössä yksilötasolla läpikäymättä jätetyt turvapiirit on lopulta käytävä läpi, mikäli yrityksen tavoitteena on samanaikaisesti säilyttää osa käytössä olevasta lukitusjärjestelmästä ja toteuttaa sen rinnalle muista järjestelmistä riippumaton turva-automaatiojärjestelmä. Tämä läpikäyntityö soveltuu paremmin projektityöksi, kuin merkittävän määrän aikaa vieväksi osaksi insinöörityön tekoa, jonka merkitys insinöörityön lopputuloksen kannalta on lopulta vähäinen.

5.2 Laitoksen riskinarviointi

Tässä luvussa tarkastetaan INEOS Composites Finland Oy:ssä tehtyä prosessin riskinarviointia, joka esitetään esimerkkipiirin korkean paineen riskin osalta liitteessä 1. Riskinarviointi on yrityksen prosessi-insinöörin haastattelun perusteella tehty hyödyntäen riskinarvioinnin tekoa varten olemassa olevaa ohjelmistoa. Koska riskinarviointi sisältää lähes 2000 riviä taulukoita, insinöörityön kannalta ei ole järkevää käydä jokaista riskinarviointia yksitellen läpi. Työmäärää supistettiin ensin rajaamalla tarkastelu pääasiassa riskeihin, joissa on tunnistettu tarve turvatoiminnolle jäännösriskin saamiseksi siedettävälle tasolle. Näiden riskien määrä oli merkittävästi pienempi. Haasteeksi insinöörityön kannalta muodostui jokaisen jo olemassa olevan turvapiirin dokumentaation määrä erityisesti piirikaavioiden osalta. Yksittäinen turvapiiri voi sisältää kymmeniä sivuja piirikaavioita, kojeluetteloita ja putkisto- ja instrumentointikaavioita. Tähän on lisättävä päälle vielä prosessien toimintakuvaukset ynnä muu sanallinen dokumentaatio. Osa dokumentaatiosta on yhteistä muiden turvapiirien kanssa. Tästä syystä päätettiin käyttää kaiken dokumentaation insinöörityöhön listauksen sijaan aikaa siihen, että löydetään riittävän hyvin kokonaisuutta edustava yksittäinen riski, johon yleistettäisiin turvajärjestelmän kokonaisuus. Riskinarvioinnin käsittely tapahtui siis tarkastelemalla yhtä tunnistettua riskiä, joka toimii insinöörityön kannalta riittävän edustavana otoksena kokonaisuudesta.

Riskinarviointi on turva-automaatiojärjestelmän toteutuksen perusta, joka on tehtävä huolellisesti. Siinä tunnistetaan riskit, arvioidaan niiden suuruudet ja näillä perustein tunnistetaan sietämättömiksi jäävät jäännösriskit, joiden alennukseen tarvitaan turvatoimintoja. Lisäksi tunnistetaan näiden jäännösriskien alentamiseksi toteutettavien tai jo toteutettujen turvatoimintojen turvallisuuden eheyden tason vaatimukset. Kaikki riskinarviointia seuraavat turva-automaatiojärjestelmän elinkaarimallin mukaiset vaiheet pohjautuvat kattavaan ja tarkkaan riskinarviointiin. Riskit, jotka ovat olemassa, mutta joita ei ole riskinarvioinnissa tunnistettu, eivät myöskään ole turva-automaatiojärjestelmän toiminnoilla turvattuja. Näin ollen laitoksen toiminnallinen turvallisuus voi jäädä puutteelliseksi.

INEOS Composites Finland Oy:llä toteutettu riskinarviointi kattaa laitoksen reaktorit 1, 2 ja 3 sekä niiden jäähdytys-, liuotus- ja sekoitussäiliöt. Lisäksi riskinarviointi kattaa pakkaustoiminnan, tuotesäiliöt, bulk-lastauksen, eräiden raaka-aineiden säilytyksen ja käsittelyn, lämmityskontin, vaarallisten kemikaalien varastoinnin, tislesäiliöt ja katalyyttisen polttolaitoksen. Riskinarviointi ei käsittele biologista puhdistuslaitosta, muiden raaka-aineiden vastaanottoa ja käsittelyä tai jauheiden käsittelyä. Jauheiden käsittelystä on olemassa oma erillinen riskinarviointi, jota ei tässä insinöörityössä käsitellä insinöörityön rajauksesta johtuen. On kuitenkin merkille pantavaa, että jauheiden käsittely on uudempi ja muusta laitoksella käytetystä teknologiasta poikkeava kokonaisuus ja sen riskinarvioinnin ja fyysisten laitteiden turva-automaatiojärjestelmään soveltuvuuden tarkastelu tulee suorittaa, kun turva-automaatiojärjestelmää aletaan suunnitella.

Toteutettu riskinarviointi on yhdistelmä HAZOP-tarkastelusta ja LOPA-menetelmästä ja se on kirjoitettu englanniksi. Riskinarviointi on toteutettu reaktorien osalta jakamalla reaktorit omiksi osuuksikseen ja käsittelemällä kunkin reaktorin eri prosessivaiheita omina riskinarvioinnin osuuksinaan.

Riskinarvioinnin prosessivaiheet erittelevän rakenteen johdosta riskinarvioinnissa tunnistetaan samoja riskejä useita kertoja, sillä monet niistä esiintyvät seurauksiltaan samoina eri prosessivaiheissa. Monessa näistä myös syyt ovat samat. Riskinarvioinnissa eniten turvatoimintoja vaativia riskejä on osittain tästä syystä tunnistettu eniten reaktoreilta ja niiden jäähdytys- ja liuotussäiliöitä. SIL 1-tason turvatoimintoja vaativia riskejä on tunnistettu yli 30, ja SIL 2-tason turvatoiminon vaativia riskejä yksi.

Riskinarvioinnissa on huomioitavaa, että vaikka reaktorit 1, 2 ja 3 ovat keskenään hyvin samankaltaiset, niin niiden riskinarviointi eroaa monelta osin merkittävästi. Riskinarvioinnin tarkastelun perusteella voidaan todeta, että HAZOP/LOPA-tiimi on kehittynyt tehtävässään riskinarvioinnin edetessä, jolloin tunnistettujen riskien arviointi on monipuolistunut ja riskejä on tunnistettu laajemmin. Toisaalta moni päälaitekokonaisuus tai sen alikokonaisuus on täysin

tyhjä, eikä näiltä osin ole voitu tunnistaa mitään mahdollisia turvatoimintotarpeita, mikäli niitä olisi

Turva-automaatiojärjestelmän tarjoama lisäys toiminnallisen turvallisuuden tasoon on riippuvainen riskinarvioinnissa havaituista turvatoimintotarpeista. Mikäli turvatoimintotarpeita ei ole kyetty havaitsemaan tai riskinarviointi on tehty puutteellisin lähtötiedoin tai -oletuksin, on sen lopputulos tulevan turva-automaatiojärjestelmän toteutusprojektin kannalta puutteellinen ja riittämättömään toiminnalliseen turvallisuuteen johtava.

5.3 Käytössä oleva turvajärjestelmä

Tässä luvussa kuvataan insinöörityön kannalta oleellisella tasolla INEOS Composites Finland Oy:ssä käytössä olevaa turvajärjestelmää. Käytössä oleva relepohjainen turvajärjestelmä, jota kutsutaan lukitusjärjestelmäksi, koostuu tunto- ja toimielimistä, apulaitteista sekä logiikkaosasta. Kunkin osakokonaisuuden laitteet käydään insinöörityöhön valitun esimerkkipiirin avulla läpi, ja tarkastetaan täyttävätkö ne niille asetetut vaatimukset kelpuutusta turva-automaatiojärjestelmässä käyttöä varten.

Reaktoreilla käytössä olevien turvapiirien toiminta on määritelty INEOS Composites Finland Oy:n lukitusdokumenteissa. Lukitusdokumentit sisältävät tiedon kunkin turvatoiminnon laukaisevista tuntoelimistä ja niiden aiheuttamat toiminnot turvapiireihin kuuluvissa toimielimissä. Lukitusjärjestelmästä ei ole koottuna yksiin kansiin dokumentaatiota, joka kattaisi elinkaarimallin kuvauksessa asetetut dokumentaation vaatimukset lukitusjärjestelmän suunnitteluperusteista, huolloista ja muutoksista ynnä muusta. Tämä koskee sekä turvapiirejä kokonaisuutena, että yksittäisiä turvalaitteita. Kojeluettelot eivät sisällä turvajärjestelmän kannalta kaikkea tarpeellista tietoa, kuten kojeiden SIL-luokituksia, laitetyyppejä tai valmistajan määrittelemää keskimääräistä vikaantumista turvatoiminnon sattuessa. Osittain tämä johtuu siitä, että turvapiireissä käytetyt laitteet eivät ole standardin IEC 61508 mukaan sertifioituja. Toisaalta myöskään laitteista, joista sertifiointi löytyy, näitä tietoja ei ole kirjattuna. Mikäli tämän kaltaista tietoa ei

haluta kirjata kojeluetteloon, tulee se dokumentoida omaan turvajärjestelmän laitekantaa käsittelevään dokumentaatioon.

5.3.1 Logiikkaosa

Logiikkaosana käytetään kolmeen eri lukituskaappiin jaoteltuja relekokonaisuuksia, ja apulaitekaappeihin sijoitettuja signaalia käsitteleviä apulaitteita. Lukituskaapeissa LK-01, LK-02 ja LK-03 on yhteensä lähes 1000 relettä. Myös releiden suuren määrän vuoksi tässä insinöörityössä ei tarkastella kaikkia olemassa olevia turvapiirejä, vaan niistä on valittu mukaan yksi kokonaisuutta riittävän hyvin edustava turvapiiri. Kaapit sisältävät myös johdonsuojakytkimiä, huolto-ohituskytkimiä ja joissain tapauksissa merkkivaloja.

Lukituskaapeissa käytettäviä relemalleja on neljää erilaista, joista kaksi mallia on kytkentäreleitä, yksi on aikarele ja yksi on jännitteenvalvontarele. Kytkentäreleiden valmistajat, mallit ja SIL-luokitukset ovat eritetty taulukossa 8.

Taulukko 8. Lukituskaapin kytkentäreleiden tiedot.

Valmistaja	**Malli**	**SIL-luokitus**
Kuhnke	UF3B-24VDCN Universal	Ei luokitusta
ComatReleco	C3-A30X 24VDC MR-C	Ei luokitusta
Selectron	GHAh	Ei luokitusta
Selectron	GZUD	Ei luokitusta

Näille releille ei ole myönnetty standardiin IEC 61508 perustuvaa SIL-luokitusta, eli ne eivät sovellu käytettäväksi turva-automaatiojärjestelmässä, mikäli turva-automaatiojärjestelmän kelpuutus tehdään reittiä 1_H pitkin, jota tämä insinöörityö käsittelee.

Apulaitekaapit sisältävät esimerkiksi ATEX Ex-luokiteltuja vahvistimia ja ATEX Ex-i-luokiteltujen turvapiirien erottimia. Yleisimpien laitteiden valmistajat, mallit ja SIL-luokitukset ovat eriteltynä taulukossa 9.

Taulukko 9. Apulaitekaappien yleisimpien laitteiden tiedot.

Valmistaja	**Malli**	**SIL-luokitus**
Pepperl+Fuchs	WE77/Ex2	Ei luokitusta
Pepperl+Fuchs	KFA6-SR2-Ex2.W	SIL 2
PR	5111 Universal Transmitter	Ei luokitusta
Stahl	9002/13-280-093-001	Ei luokitusta

Pepperl+Fuchs KFA6-SR2-Ex2.W on SIL-luokiteltu SIL 2-tasolle asti [39]. Muilla tarkastetuilla laitteilla ei ole SIL-luokitusta. On mahdollista, että apulaitekaapeissa on yksittäisiä laitteita, joilla on SIL-luokitus, joita ei tarkastettu. Insinöörityön kokonaisuuden kannalta tällä ei kuitenkaan ole merkittävää vaikutusta. Apulaitekaapeissa sijaitsevien SIL-luokiteltujen ja ei-SIL-luokiteltujen laitteiden yhtäaikainen olemassaolo turvapiireissä on trendi, joka vallitsee myös muilla lukitusjärjestelmän fyysisillä tasoilla.

5.3.2 Kenttälaitteet

INEOS Composites Finland Oy:llä on käytössä laajasti erilaisia kenttälaitteita useilta eri vuosikymmeniltä. Tehdasta on laajennettu useissa eri projekteissa, joiden myötä myös käytössä olevien laitteiden laitekanta on laajentunut. Tiettyjen laitteiden, kuten venttiilien, pumppujen ja yksinkertaisten instrumenttien osalta laitekanta on melko yhdenmukaista. Tämä helpottaa esimerkiksi kunnossapito-organisaation työtä pienentämällä varastossa olevien erilaisten varaosien määrää. Toisaalta joidenkin projektien osalta laitekannan monimuotoisuus on laajentunut, eikä näitä laitteita käytetä muualla kuin kyseisissä projekteissa rakennetuissa kokonaisuuksissa. Esimerkiksi jauheidensiirtokokonaisuuden

osalta käytössä oleva laitekanta on hyvin erilaista kuin muu tehtaalla käytössä oleva laitteisto.

Insinöörityössä suoritetun tarkastelun perusteella osalla kenttälaitteista on standardin IEC 61508 mukainen SIL-luokitus. Kyseisiä laitteita ei näyttäisi olevan valittu lukitusjärjestelmän tai käyttöautomaatiojärjestelmän piireihin näiden perusteilla, sillä muilla piireihin kuuluvilla laitteilla sertifiointia ei välttämättä ole. SIL-luokiteltujen laitteiden valinta piireihin vaikuttaa epäjohdonmukaiselta, eikä niiden tarpeellisuutta ole kenties aina tunnistettu lukitusjärjestelmään liittyvien turvapiirien laitevalintoja tehtäessä. Turvapiirien kenttälaitteista löytyy sekä monimutkaisempia elektronisia mittalaitteita, että yksinkertaisempia kytkimiä. Nämä edustaisivat siis A- ja B-laitetyyppejä, mikäli ne olisivat määritelty.

Kahdennettuja mittauksia löytyy pääasiassa lämpötilamittauspiireistä, joiden tuntoelimet ovat usein kahdennettuja PT-100-mallisia lämpötila-antureita HART-lähettimillä varustettuna. Kahdennus esitetään mittalaitteiden positioissa A- ja B-päätteillä. Näissä piireissä kahdennus kohdistuu myös kaapelointiin, liittimiin ja käyttöautomaatiojärjestelmän IO-korttien kanaville.

5.3.3 Esimerkkipiiri

Edellä mainituista syistä johtuen insinöörityössä tarkasteltavaksi valittu turvapiiri on reaktorin DC-81601 korkeasta paineesta painekytkimellä PSA-81605, korkeasta lämpötilasta lämpötilamittauksillaTICA-81601 tai TIZ-81659 tai liian alhaisesta sekoittimen pyörimisnopeudesta nopeusvahdilla XSA-81620 venttiilin XCV-816103 sulkeva turvapiiri. Turvatoiminnon laukaisee ja venttiilin XCV-816013 sulkee myös hätäpysäytyskytkimet SW-81603 ja SW-81605. Kyseiset tuntoelimet ohjaavat logiikkayksikön kautta myös muita toimielimiä. Nämä muut toiminnot eivät ulotu tämän insinöörityön tarkasteluun. Niiden fyysinen rakenne ja arkkitehtuuri ei eroa merkittävästi tarkasteltavasta turvapiiristä, eikä niiden tarkastelu toisi näin ollen merkittävää lisäarvoa insinöörityöhön. Tarkasteltavan turvapiirin lukitusdokumentti on liitteessä 2.

Kenttälaitteet

Valitun esimerkkipiirin tuntoelimiin kuuluvat PSA-81605, TICA-81601 ja TIZ-81659. Toimielimistä esimerkkipiiriin kuuluu venttiili XCV-816103 ja paineilman virtausta venttiilin toimilaitteelle ohjaava solenoidiventtiili XYV-816103. Lisäksi esimerkkipiiriin kuuluvat hätäpysäytyskytkimet SW-81603 ja SW-81605, lämpötilalukituksen kuittauskytkin SW-81683 ja painelukituksen kuittauskytkin SW-81611. Piiriin kuuluu myös reaktorin sekoittimen GD-81601 pyörimisnopeuden vahti XSA-81620, josta ei ole olemassa tarkempia tietoja. Tuntoelimien valmistajat, mallit ja SIL-luokitukset esitetään taulukossa 10.

Taulukko 10. Erimerkkipiirin tuntoelimien tiedot.

Valmistaja	**Malli**	**SIL-luokitus**
Beta	V3-V504H-S1N-S2-Z1	SIL 2
SKS	2xWT-BH-12-DAN-405/207-4J-KLA	Ei luokiteltu
PR electronics	PR5331B3B	Ei luokiteltu

Tyyppiä B oleva kytkin PSA-81605 on Betan valmistama painekytkin. Tämän painekytkimen turvallisuuden eheyden taso on SIL 2 [40]. Painekytkimen kojeluettelotiedot esitetään liitteessä 3. TICA-81601 ja TIZ-81659 ovat SKS:n valmistamia lämpötilamittareita, joissa on PR electronicsin valmistamat HART-lämpötilalähettimet. Lämpötilamittarilla tai lämpötilalähettimellä ei ole SIL-luokitusta. TICA-81601:n kojeluettelotiedot esitetään liitteessä 4, ja TIZ-81659:n kojeluettelotiedot esitetään liitteessä 5.

Venttiilikokonaisuus XCV-816103 koostuu tulppaventtiilistä, toimilaitteesta, solenoidiventtiilistä ja asennoittimesta. Näiden komponenttien valmistajat, mallit ja SIL-luokitukset esitetään liitteessä 11.

Taulukko 11. Esimerkkipiirin venttiilin komponenttien tiedot.

Valmistaja	Malli	Kuvaus	SIL-luokitus
Elomatic	ES200/5	Toimilaite	Ei luokiteltu
Emerson/Elomatic	HDX H2	Asennoitin	Ei luokiteltu
3Z	120 FS	Tulppaventtiili	Ei luokiteltu

Venttiilikokonaisuus on tilattu kohteeseen Klingeriltä, joka on toimittanut suuren osan tehtaalla käyteytyistä venttiileistä. Venttiilin komponentteja ei ole SIL-luokiteltu Venttiilikokonaisuuden XCV-816103 kojeluettelotiedot löytyvät liitteestä 6.

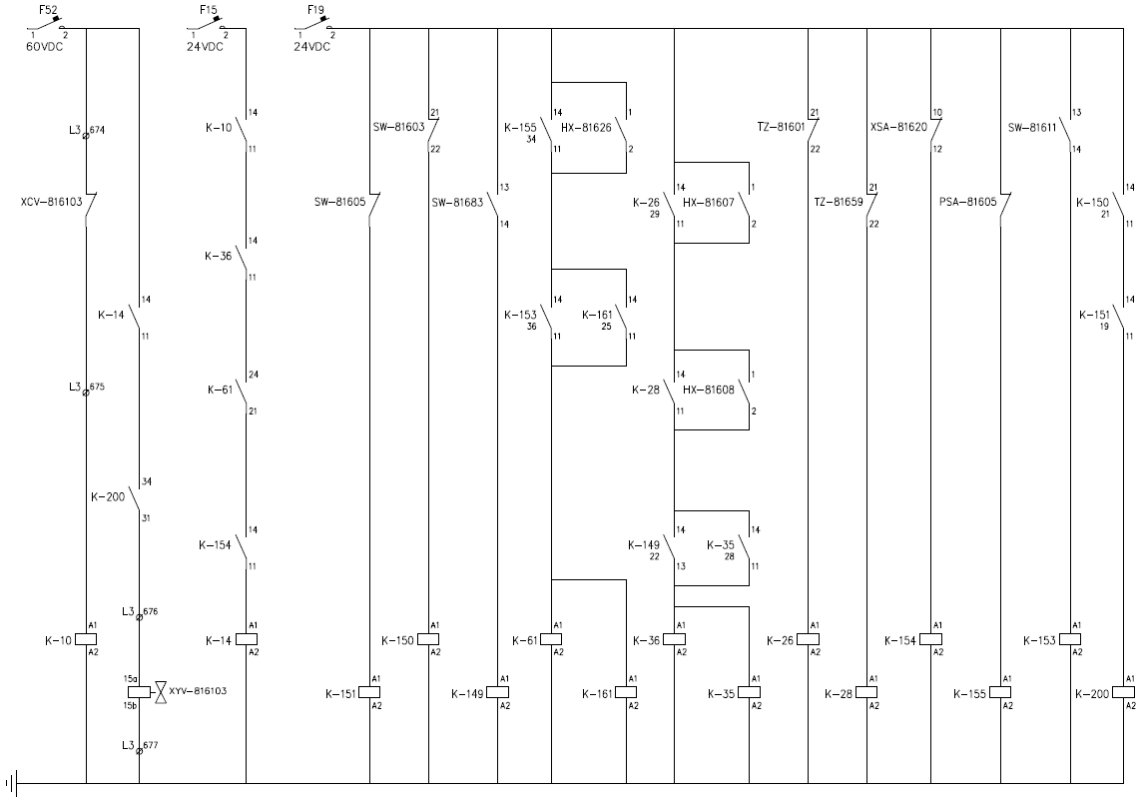
Sähkövirta ohjaa sähkömagneetin avulla suuntaventtiilin asentoon, jossa se päästää paineilman virtaamaan toimilaitteelle suuntaventtiilin läpi. Tällöin toimilaite kääntää paineilman avulla tulppaventtiilin XCV-816103 auki. Kun sähkövirta katkeaa suuntaventtiilin sähkömagneetista, niin suuntaventtiilin asennon muuttuessa myös paineilman virtaus toimilaitteelle katkeaa. Tällöin toimilaitteen jousi palauttaa venttiilin kiinni-asentoon ja toimilaitteessa ollut paineilma purkautuu suuntaventtiilin kautta ulos. Käyttöautomaatiojärjestelmällä ohjataan sähkövirran kulkua suuntaventtiilin sähkömagneetille lukitusjärjestelmän releiden kautta.

Hätäpysäytyskytkimet sijaitsevat lähellä reaktoria kentällä. Ne ovat Stahlin valmistamia 8020/22-hätäpysäytyskytkimiä. Turvatoimintojen nollauskytkimet ovat kuittauspaneelissa olevia jousipalautteisia kytkimiä. Näiden SIL-luokituksista ei ole tietoa.

Logiikkaosa

Esimerkkipiirin logiikkaosassa 15 relettä. Liitteissä 7 esitetään relelogiikkan virtapiirikaavio. Kuva 2 on insinöörityötä varten laadittu yhteenveto näistä virtapiirikaavioista. Kuvassa 2 osa virtapiirikaavioiden tiedoista, kuten liittimistä, on

tarkoituksellisesti jätetty pois. Kuva 2 löytyy suurempana liitteestä 8.



Kuva 2. Esimerkkipiirin virtapiirikaavio.

Kuvassa 2 relettä K-10 ohjaavan piriin liittimet L3:674 ja L3:675 ovat käyttöautomaatiojärjestelmän prosessiaseman PA6 binääriulostulokortin 01BOU kanavaan 01 kiinnittyvät liittimet, joilla ohjataan kuvassa näkyvän koskettimen XCV-816103 asentoa. Liitteen 7 sivulla 1 löytyy venttiilin XCV-816103 virtapiirikaavio, jossa nämä liittimet myös näkyvät. Käyttöautomaatiojärjestelmällä ohjataan siis lukitusjärjestelmässä olevan releen K-10 tilaa, ei suoraan venttiilin XCV-816103 asentoa. Toiminta on tältä osin lepovirtaperiaatteella toimiva, jolloin käyttöautomaatiojärjestelmän puoleinen virtapiirin vikaantuminen on turvallista sulkien venttiilin XCV-816103.

Kuvassa 2 olevat liittimet L3:676 ja L3:677 ovat venttiiliä XCV-816103 ohjaavan solenoidiventtiilin XYV-816103 pään liittimet. Liitteen 7 sivulla 1 näkyvät myös nämä liittimet. Jotta käyttöautomaatiojärjestelmästä tehty pyyntö avata venttiili

XCV-816103 myös avaisi sen, on releiden K-14 ja K-200 vetää. Tällöin 60 VDC sähkö virtaa solenoidiventtiilille XYV-816103 avaten venttiilin XCV-816103.

Rele K-14 vastaa tuntoelimien tilatietojen valvonnasta. Mikäli paine- tai lämpötilalukitukset laukeaisivat tuntoelimillä PSA-81605, TZ-81601 tai TZ-81659, päästäisi rele K-14 alareleiden ketjutuksen kautta. Rele K-36 valvoo lämpötilamittareiden tilatietoa ja rele K-61 valvoo painekytkimen tilatietoa. Pyörimisnopeusvahti XSA-81620 estää liian alhaisen pyörimisnopeuden tilassa releen K-14 vedon. Kullakin tuntoelimellä, paitsi pyörimisnopeusvahdilla XSA-81620, on lisäksi oma huolto- ja kuittauskytkin releineen. Huoltokytkimet ovat HX-816-alkuisia positioita ja kuittauskytkimet ovat normaalisti avoimia SW-816-alkuisia positioita. Tuntoelimien kytkimet ovat virtapiirikaavioiden mukaan normaalisti kiinni. Tällöin vaaditaan kytkimen avautuminen, jotta piiri aukeaa. Tuntoelimien kytkimien aukeaminen tapahtuu, kun prosessin tila muuttuu vaaralliseksi.

Rele K-200 vastaa hätäpysäytyskytkimien tilatietojen valvonnasta. Mikäli hätäpysäytyskytkimien SW-81603 tai SW-81605 virtapiiri avataan kytkintä kääntämällä, päästää rele K-200 ja venttiili XCV-816103 sulkeutuu. Hätäpysäytyskytkimien piirit toimivat lepovirtaperiaatteella, eli niiden piiriviat aiheuttavat turvallisen vikaantumisen laukaisten turvatoiminnon.

5.4 Esimerkkipiirin turvallisuuden eheyden taso ja vikasietoisuus

Turvallisuuden eheyden taso ilmoitetaan SIL-arvona. Turvapiirin SIL-luokitus määrittyy valmistajien laitteilleen määrittämien PFD_{avg}-arvojen ja turvapiirin vikasietoisuuden vaatimuksen perusteella. Koska kaikille turvapiiriin kuuluville laitteille ei ole määritelty PFD_{avg}-arvoja, niin turvapiireille ei voida kelpoistusreitin 1_H perusteella määritellä SIL-tasoja ja systemaattisen kyvykkyyden osoittaminen on mahdotonta.

Turvapiirien arkkitehtuuri on painemittauspiirissä PSA-81605 äänestysrakennetta 1oo1. Lämpötilamittauspiireissä TZ-81601 ja TZ-81659 on käytössä 1oo2-

äänestysrakenne. Tällä ei ole esimerkkipiirin turvallisuuden eheyden tason määrityksen osalta merkitystä laitteiden PFD_{avg}-arvojen puuttuessa.

5.4.1 Turvajärjestelmän erillisyys

Tehtaalla käytössä oleva lukitusjärjestelmä on osa käyttöautomaatiojärjestelmän turvallisuuden kannalta kriittisiksi tunnistettuja säätöpiirejä, kuten tarkasteltavaa esimerkkipiiriä. Lukitusjärjestelmän releketju ohjaa venttiilin XCV-816103 kiinni, mikäli prosessi ajautuu vaaralliseen tilaan huolimatta siitä, antaako käyttöautomaatiojärjestelmä pyynnön kyseisen venttiilin avaukselle. Käyttöautomaatiojärjestelmä ei siis ohjaa kyseistä venttiiliä suoraan, vaan kuittaa yhden osan lukitusjärjestelmän lukitusketjua. Tämä ilmenee liitteessä 7.

Lähtökohtaisesti käyttöautomaatiojärjestelmän ei kuitenkaan tulisi antaa kirjoittaa mitään turvajärjestelmään. Tästä syystä olisi selkeää, mikäli vain turvajärjestelmästä ohjattaisiin turvajärjestelmään kuuluvaa venttiiliä. Aina tämä ei kuitenkaan ole mahdollista, sillä tämä vaatisi omat venttiilit turva- ja käyttöautomaatiojärjestelmien ohjauksille. Tämänkaltainen toteutus vaatii suunnittelua, mahdollisia painelaitemuutoksia ja investointeja kenttälaitteisiin. Toteutus tekisi jo valmiiksi ahtaasta prosessiympäristöstä vieläkin ahtaamman ja epäergonomisemman. Käytännössä toteutus, jossa turvajärjestelmän ohjaus on aina korkeamman prioriteetin ohjaus kuin käyttöautomaatiojärjestelmän, ja joka voidaan luotettavasti ja aukottomasti osoittaa näin toimivan, on tehokkain ratkaisu. Tämä asia tulee käydä turva-automaatiojärjestelmän toimittajan kanssa läpi.

6 Yhteenveto

Työn tavoitteena oli selvittää, mitä lukitusjärjestelmällä toteutettavia turvatoimintovaatimuksia oli tunnistettu prosessin riskinarvioinnissa ja mitkä niiden turvallisuuden eheyden tason vaatimukset olivat. Tämän jälkeen oli tarkoitus tutustua tehtaan lukitusjärjestelmän arkkitehtuuriin ja yksittäisten turvatoimintojen toteutukseen. Tarkoituksena oli saada kuva siitä, toteutuivatko riskinarvioinnissa vaaditut turvallisuuden eheyden tason vaatimukset käytännön turvatoimintojen toteutuksissa. Toisena tavoitteena on antaa suosituksia, kuinka tulisi edetä turva-automaatiojärjestelmän toteutuksessa.

Lukitusjärjestelmän ominaisuuksien selvitystyö aloitettiin tarkastelemalla laitoksesta tehtyä riskinarviointia. Riskinarvioinnin tarkastelussa keskityttiin pääasiassa niihin tunnistettuihin riskeihin, joiden jäännösriski ennen turva-automaatiotoimintojen huomioimista oli sietämättömällä tasolla. Näiden riskien osalta tarkasteltiin olemassa olevien turvatoimintojen piirikaavioita, kojeluetteloita sekä putkisto- ja instrumentointikaavioita. Lisäksi tarkasteltiin turvajärjestelmästä ja prosessista olemassa olevaa dokumentaatiota. Insinöörityössä etsittiin yleisesti turvajärjestelmää kattavasti edustava turvapiiri, joka turvasi useita prosessilaitteita, käytti muissakin turvatoiminnoissa käytettäviä tunto- ja toimielimiä sekä signaalin käsittelyyn liittyviä apulaitteita ja kuittauskytkimiä.

Turva-automaatiojärjestelmän toteutus pohjautuu elinkaarimallin mukaisesti tehtaan riskinarviointiin. Tästä syystä ennen uuden turva-automaatiojärjestelmän rakentamista tulisi suorittaa uusi HAZOP-tarkastelu ja LOPA-menettely, jonka kautta tunnistetaan tulevan turva-automaatiojärjestelmän turvatoimintojen tarpeet. Tarkastelu tulisi suorittaa siitä lähtökohdasta, että mitään turvallisuuden eheyden tason vaatimuksen täyttäviä turvapiirejä ei nykyisessä lukitusjärjestelmässä ole olemassa, eikä niitä tällöin oteta huomioon riskejä alentavasti. HAZOP- ja LOPA-tiimien jäseniksi on suositeltavaa ottaa kunnossapidon instrumenttiasentaja, kokenut operaattori ja / tai vuoromestari, tuotannonsuunnittelija, käyttöinsinööri, tuotantopäällikkö, SHE-insinööri (Safety, Health and Environment) ja henkilö, jolla on käytännön kokemusta tarkasteltavana olevan

prosessin ohjauksesta sekä tarvittaessa toimitusketjujen päällikkö. Käytännön kokemuksen omaava henkilö voi olla konsultti tai aikaisemmin vastaavaan tutkintaan osallistunut henkilö. Tärkeintä on ennen aloitusta hahmottaa toivottu lopputuloksen malli.

Riskinarvioinnissa tunnistettujen turvapiirien vaateiden määrä vaikuttaa turva-automaatiojärjestelmän logiikkaosan valintaan. Logiikkaosan valinta on suositeltavaa suorittaa yhteistyössä käyttöautomaatiojärjestelmän toimittajan kanssa, jotta kommunikaatio turva-automaatiojärjestelmästä käyttöautomaatiojärjestelmään toimii. Tilatietojen, hälytysten ynnä muiden tarpeellisten tietojen välitys turva-automaatiojärjestelmästä käyttöautomaatiojärjestelmään on saatava suoritettua vaarantamatta turva-automaatiojärjestelmän riittävää eriytysvaatimusta eli turvatoimintojen suoritusta vaateesta.

Turva-automaatiojärjestelmän logiikkayksikkö, joka voi olla esimerkiksi ohjelmoitava logiikka (Programmable Logic Controller, PLC), korvaa nykyisin käytössä olevan relepohjaisen lukitusjärjestelmän turvallisuuden eheyden tasoa vaativien turvatoimintojen osalta. Kun mietitään turva-automaatiojärjestelmän kahdennuksia, on syytä harkita vähintään sekä logiikkayksikön ja tehonsyötön kahdennuksia.

Nykyinen käyttöautomaatiojärjestelmä on teknologialtaan käyttöikänsä päässä. Varaosien valmistus järjestelmää varten on osittain jo päättynyt, ja tulee päättymään täysin tulevien vuosien aikana. Tässä vaiheessa jälkimarkkinoilta saatavat, mahdollisesti käytetyt varaosat ovat ainoa varaosien lähde. Siirtymällä ohjelmoitavaan logiikkaan pohjautuvaan turva-automaatiojärjestelmään vapautuu käyttöautomaatiojärjestelmästä prosessiasemilta nyt käytössä olevia ja toimivia kanavapaikkoja varalle.

Ne turvapiirit, jotka ovat olemassa nykyisessä lukitusjärjestelmässä, ja joita ei riskinarvioinnin tulosten perusteella tarvitse toteuttaa turvatoiminnoilla, voivat jäädä nykyiseen käytössä olevaan lukitusjärjestelmään osaksi käyttöautomaatiojärjestelmää. Nämä piirit ovat kuitenkin erotettava turva-

automaatiojärjestelmän turvapiireistä kaikessa dokumentaatiossa. Nykyisen relepohjaisen lukitusjärjestelmän piireille ei voida määritellä suoraan turvallisuuden eheyden tasoja, jolloin niillä ei ole riskiä alentavaa vaikutusta riskinarviointia suoritettaessa.

Mikäli osalle nyt käytössä olevalle laitteistolle on valmistaja antanut mahdollisuuden määrittää sen turvallisuuden eheyden tason reittiä 2_H pitkin, voidaan nämä laitteet säilyttää. Reitti 2_H perustuu loppukäyttäjältä saatuihin komponenttien luotettavuustietoihin, joten vikaantumishistoria näiden laitteiden osalta tulee olla luotettavasti dokumentoitu [32, s. 42]. Reittiä 2_H käytettäessä tulee turvautua ulkopuoliseen asiantuntija-apuun testausten ja korkeampien luotettavuustasojen määrittelyn osalta.

Jotta riskinarvioinnissa tunnistetuille turvatoimintotarpeille voitaisiin määritellä turvallisuuden eheyden taso, on näihin turvapiireihin kuuluvien laitteiden täytettävä niille asetetut vaatimukset kokonaisuutena. Tämä tarkoittaa turva-automaatiojärjestelmään siirrettävien turvapiirien osalta kenttälaitteiden vaihtoa SIL-luokiteltuihin kenttälaitteisiin niiden osalta, joille valmistaja ei ole reitin 1_H kannalta vaadittavia tietoja. Koska nykyisessä riskinarvioinnissa tunnistetut turvapiiritarpeet ovat SIL-tasoltaan pääosin matalinta SIL 1-tasoa, ei laitteiden tarvitse tai kannata olla monimutkaisia A-tyypin laitteita, mikäli mahdollista. Oikealla laitevalinnalla turvapiirin vikasietoisuudeksi riittää 0, ja äänestysrakenteeksi kaikista yksinkertaisin 1oo1. Mikäli 1oo1-äänestysrakenteen heikko vikasietoisuus nähdään itsessään liian merkittävänä ongelmana, on syytä harkita redundanttisempaa äänestysrakennetta, kuten 1oo2. Tällöin kenttälaitteiden kahdennuksessa on syytä harkita redundanttisuuden kasvattamista käyttämällä eri valmistajien laitteita tai esimerkiksi eri teknologiaan perustuvia laitteita.

Nykyisiä kenttälaitteita on syytä hyödyntää uusia kenttälaitteita valittaessa putkisto- ja muiden muutosten minimoimiseksi. Yksinkertaisin ratkaisu vaatimukset täyttäviä kenttälaitteita hankittaessa on säilyttää sama koko- ja paineluokka, materiaali, ATEX-luokitus, liittimien koko ja määrä sekä mahdollisuuksien mukaan sama kaapelointi, signaalityyppi ja jänniteluokka.

Purkamalla nykyisiä lukitusjärjestelmän piirejä muutoksia tehdessä kentältä kytkentäkotelosta ja kytkentähuoneesta ristikytkentäkaapista voidaan säilyttää nykyinen runkokaapelointi ja kytkennät kytkentähuoneessa soveltuvilta osin. Kytkentähuoneesta on mahdollista purkaa kytkentöjä automaatiojärjestelmästä päin katsottuna ennen apulaitekaappeja olevasta ristikytkennästä. Tällöin piireille tarpeelliset barrierit ATEX Ex-i luokituksineen ynnä muut apulaitteet säilyvät kytkennöiltään muuttumattomina.

Elinkaarimallin vaatimusten mukaisesti joka elinkaaren vaihe on dokumentoitava, jotta turva-automaatiojärjestelmä voidaan kelpuuttaa sille asetetut vaatimukset täyttäväksi. Elinkaarimallin vaiheista tuotettu dokumentaatio tulee kasata omaksi kokonaisuudekseen painelaitekansioiden tapaan. Tarvittavan dokumentaation määrittelyssä voidaan turvautua turva-automaatiojärjestelmän toimittajan apuun.

Niiltä osin, kuin turvapiirejä siirretään nykyisestä lukitusjärjestelmästä toteutettavaan turva-automaatiojärjestelmään, on piirien puruista huolehdittava elinkaarimallin mukaisesti. Niiden käytöstä poisto on tehtävä huolellisesti prosessin turvallisuutta vaarantamatta ja kaikki niihin liittyvä dokumentointi on päivitettävä. Tätä ei voida suorittaa prosessin käydessä, joten pidempiaikainen tuotantolinjan pysäytys tai vuotuinen huoltoseisokki ovat hyviä aikoja muutosten toteuttamiselle.

Lähteet

1 Ineos Composites Finland Oy. 2022. Verkkoaineisto. Kilpilahti. <https://www.kilpilahti.fi/yritys/ineos-composites-finland-oy/>. Luettu 9.1.2022.

2 Ineos Composites Finland Oy. 2020. Verkkoaineisto. Finder. <https://www.finder.fi/Muovin+raaka-aineet/Ineos+Composites+Finland+Oy/Porvoo/yhteystiedot/191861>. Luettu 9.1.2022.

3 About. 2022. Verkkoaineisto. INEOS Group Ltd. <https://www.ineos.com/about/>. Luettu 9.1.2022.

4 Markets. 2022. Verkkoaineisto. INEOS Group Ltd. <https://www.ineos.com/businesses/ineos-enterprises/businesses/ineos-composites/markets/>. Luettu 9.1.2022.

5 EU:n päätökset, asetukset ja direktiivit. 2013. Verkkoaineisto. Selko.fi. <https://www.ineos.com/businesses/ineos-enterprises/businesses/ineos-composites/markets/>. Päivitetty 2.12.2013. Luettu 9.1.2022.

6 Direktiivi 2006/42/EY: Euroopan parlamentin ja neuvoston direktiivi koneista ja direktiivin 95/16/EY muuttamisesta. 2006. Euroopan unionin virallinen lehti 9.6.2006. <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32006L0042&from=FI>.

7 Direktiivi 2014/35/EU: Euroopan parlamentin ja neuvoston direktiivi tietyllä jännitealueella toimivien sähkölaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta. 2014. Euroopan unionin virallinen lehti 29.3.2014. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32014L0035>.

8 Direktiivi 2014/30/EU: Euroopan parlamentin ja neuvoston direktiivi sähkömagneettista yhteensopivuutta koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta. 2014. Euroopan unionin virallinen lehti 29.3.2014. <https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX%3A32014L0030>.

9 Direktiivi 2014/34/EU: Euroopan parlamentin ja neuvoston direktiivi räjähdysvaarallisissa tiloissa käytettäviksi tarkoitettuja laitteita ja suojajärjestelmiä koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta. 2014. Euroopan unionin virallinen lehti 29.3.2014. <https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX%3A32014L0034>.

10 Direktiivi 2014/68/EU: Euroopan parlamentin ja neuvoston direktiivi painelaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta. 2014. Euroopan unionin virallinen lehti 27.6.2014. <https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX%3A32014L0068>.

11 Lainsäädäntö. 2022. Verkkoaineisto. Eduskunta. <https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx/>. Luettu 9.1.2022.

12 Työturvallisuuslaki. 2002. 738/23.8.2002.

13 Laki räjähdysvaarallisissa tiloissa käytettäväksi tarkoitettujen laitteiden ja suojausjärjestelmien vaatimustenmukaisuudesta. 2016. 1139/16.12.2016.

14 Lait, asetukset, määräykset yms. 2022. Verkkoaineisto. Vandernet. <https://www.vandernet.com/teollisuus/content/lait-asetukset-määräykset-yms/>. Luettu 9.1.2022.

15 Valtioneuvoston asetus koneiden turvallisuudesta. 2008. 400/2008.

16 Valtioneuvoston asetus vaarallisten kemikaalien käsittelyn ja varastoinnin valvonnasta. 2015. 685/2015.

17 Valtioneuvoston asetus vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista. 2012. 856/2012.

18 Valtioneuvoston asetus räjähdyskelpoisten ilmaseosten työntekijöille aiheuttaman vaaran torjunnasta. 2003. 576/2003.

19 Mitä standardi tarkoittaa? 2022. Verkkoaineisto. Suomen Standardoimisliitto SFS ry. <https://sfs.fi/standardeista/mika-on-standardi//>. Luettu 9.1.2022.

20 SFS-EN 61508-1. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset. 2011. Helsinki: Suomen Standardoimisliitto SFS ry.

21 SFS-EN 61511-1. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset. 2017. Helsinki: Suomen Standardoimisliitto SFS ry.

22 SFS-EN 61508-0. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 0:

Toiminnallinen turvallisuus ja IEC 61508. 2011. Helsinki: Suomen Standardoimisliitto SFS ry.

23 SIL, Osa 2: Arkkitehtuurin rajoitteet. 2022. Verkkoaineisto. PR electronics. <https://www.prelectronics.com/fi/support/pr-knowledge-library/tips-and-tricks/sil-osa-2-arkkitehtuurin-rajoitteet/>. Luettu 9.1.2022.

24 SFS-EN 61508-4. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 4: Määritelmät ja lyhenteet. 2010. Helsinki: Suomen Standardoimisliitto SFS ry.

25 Korhonen, Juha. 2011. Satunnaisvikaantumisten hallinta ja lasketa. Verkkoaineisto. ÅF-Consult Oy. <https://www.automaatioseura.fi/site/assets/files/1431/asaf_teema_2_sas_turvallisuus_-_teemap_juha_korhonen_-consult.pdf>.7.11.2011. Luettu 9.1.2022.

26 Releiden käyttö rautatieturvalaitetekniikassa. 2013. Verkkoaineisto. Liikennevirasto. <https://julkaisut.vayla.fi/pdf3/lop_2013-05_releiden_kaytto_web.pdf>.Luettu 9.1.2022.

27 SFS-EN 61511-3. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 3: Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiseen. 2017. Helsinki: Suomen Standardoimisliitto SFS ry.

28 SFS-EN 61511-4. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 4: Selitykset ja perustelut standardin IEC 61511-1 ensimmäisen ja toisen painoksen välillä tehdyille muutoksille. 2020. Helsinki: Suomen Standardoimisliitto SFS ry.

29 SFS-EN 61508-5. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tason määrittämiseksi. 2011. Helsinki: Suomen Standardoimisliitto SFS ry.

30 Pelastuslaki. 2011. 379/29.4.2011.

31 Matinaho, Sami. 2019. Systeemitekniikka TX00CY39-3001: Turva-automaatio. Luentomoniste: Opetuskerta 1. Metropolia Ammattikorkeakoulu.

32 SFS-EN 61508-2. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille. 2011. Helsinki: Suomen Standardoimisliitto SFS ry.

33 SIL, Osa 1: Satunnainen laitteiston eheys. 2022. Verkkoaineisto. PR electronics. <https://www.prelectronics.com/fi/support/pr-knowledge-library/tips-and-tricks/sil-osa-1-satunnainen-laitteiston-eheys/>.Luettu 10.1.2022.

34 Sundquist, Matti. Toiminnallinen turvallisuus: periaatteet. 2022. Verkkoaineisto. Sundcon Oy. <https://www.automaatioseura.fi/site/assets/files/1431/asaf_teema_1_2011_jestelmsuunnittelu_171011.pdf>. Luettu 10.1.2022.

35 Lundteigen, Mary Ann; Rausand, Marvin. Chapter 8. PFD formulas in IEC 61508. 2022. Verkkoaineisto. RAMS Group. <https://www.ntnu.edu/documents/624876/1277046207/SIS+book+-+chapter+08+-+PFDavg+with+IEC+61508+formulas/0be9ac0d-7e57-4641-9043-7d2554c16cac>.Luettu 10.1.2022.

36 SIL, Osa 3: Systemaattinen kyvykkyys. 2022. Verkkoaineisto. PR electronics. <https://www.prelectronics.com/fi/support/pr-knowledge-library/tips-and-tricks/sil-osa-3-systemaattinen-kyvykkyys/>.Luettu 9.1.2022.

37 SFS-EN 61511-2. Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 2: Ohjeita standardin IEC 61511-1:2016 soveltamiseen. 2017. Helsinki: Suomen Standardoimisliitto SFS ry.

38 Matinaho, Sami. 2019. Systeemitekniikka TX00CY39-3001: Turva-automaatio. Luentomoniste: Opetuskerta 3. Metropolia Ammattikorkeakoulu.

39 Switch Amplifier KFA6-SR2-Ex2.W. Verkkoaineisto. Pepperl+Fuchs. <https://www.pepperl-fuchs.com/finland/fi/classid_6.htm?view=productdetails&prodid=3138>.Luettu 10.1.2022.

40 Pressure and Temperature Switches. 2022. Verkkoaineisto. Beta. <https://beta-b.nl/wp-content/uploads/2021/02/02122020-Gen.-Cat.-Europe..pdf)>. Luettu 10.1.2022.

41 20181120 Porvoo_HAZOP-LOPA D. 2018. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

42 P4-3907-0001, muutos 10. 2005. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

43 P4-2185-0122, muutos 26. 2020. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

44 P4-2185-0051, muutos 36. 2004. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

45 P4-2185-0068, muutos 45. 2004. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

46 P4-2185-0651, muutos 37. 2006. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

47 P3-9600-0963, muutos 53. 2006. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

48 P3-5485-0171, muutos 26. 2015. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

49 P3-5485-0172, muutos 19. 2006. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

50 P3-5485-0105, muutos 30. 2019. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

51 P3-5485-0108, muutos 30. 2019. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

52 P3-5485-0166, muutos 19. 2006. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

53 P3-5485-0165, muutos 17. 2005. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

54 P3-5485-0106, muutos 19. 2006. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

55 P3-5485-0107, muutos 30. 2019. Yrityksen sisäinen dokumentti. INEOS Composites Finland Oy.

Riskinarviointi: Korkea paine reaktorilla DC-81601

Tämä liite sisältää INEOS Composites Finland Oy:ssä tehdyn riskinarvioinnin reaktorin DC-86101 liian korkeasta paineesta. Riskinarvio on jaettu seitsemään osaan, joista seuraava osa jatkaa suoraan edellistä osaa.

Taulukko 1. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 1/6 [41].

Study Node: 2. Reactor 1
Design Intent: 14. Normal process

ID	Deviation Parameter	Deviation Guide Word	Causes	Consequences	Severity
1.	Temperature	1. More, High, Long	1. Failure of the reactor temperature control loop	1. Inadvertent heating of the batch to auto-exotherm, beginning at about 245°C. Decarboxylation reaction, high reactor temperature, high reactor pressure, rupture of the reactor. Multiple on-site fatalities.	1

Taulukko 2. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 2/6 [41].

Initiating Event		Enabling Event Modifiers / Conditional Modifiers			Time at Risk	
Initiating Event	F	No.	Description	Prob	Events/Year	Per Event (h)
Basic Process Control System (BPCS) - Control Loop Failure	1,00E-01	1.	Probability of a Person Being Present in the Area Affected by the Event: Routinely Monitored, Visited or Occupied Area	1,00E+00	454	7

Taulukko 3. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 3/6 [41].

Unmitigated Risk			
Rationale	**F Calc**	**F Round**	**R**
	3,63E-02	1,00E-01	Immediate

Taulukko 4. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 4/6 [41].

As-Is Risk				As-Is Risk
No.	**Existing IPLs**	**Indiv PFOD**	**Rationale**	**Existing Safeguards**
1.	Other Safeguard	1,00E+00	Venting (including rupture disc) is not an IPL. Insufficient venting for the second runaway reaction.	1. Venting (including rupture disc) is not an IPL. Insufficient venting for the second runaway reaction.
2.	Other Safeguard	1,00E+00	Existing SIS is not independent from BPCS. No IPL credit can be applied.	
3.	Other IPL, 1.0E-01	1,00E-01	cooling tank	

Taulukko 5. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 5/6 [41].

As-Is Risk	
F	**R**
1,00E-02	Immediate

Taulukko 6. Riskinarvio reaktorin DC-81601 korkeasta paineesta, osa 6/6 [41].

Revised Risk					
No.	**Recommended Safeguard/IPL**	**Indiv PFOD**	**Rationale**	**F**	**R**
1.	SIL (Safety Integrity Level) 1 System	1,00E-01		1,00E-05	Optional
2.	Other Safeguard	1,00E+00	Independent alarm not associated with the BPCS. This is a dedicated alarm and evacuation to reduce severity. A written plan is available and the site conducts evacuation drills. Per guidelines, evacuation is a safeguard, not an IPL.		
3.	Human Response to an Annunciator (Light and Audio), 2 to 10 Minutes of Response Time Available.	1,00E-01	Operator closes a single, manual hot-oil valve. It cannot be the same operator who closes the two cooling valves. Secondary sign-off needed. Training required.		
4.	Human Response to an Annunciator (Light and Audio), 2 to 10 Minutes of Response Time Available.	1,00E-01	Operator can close a single, manual instrument air valve to force cooling valves to open. This cannot be the same operator who closes the manual hot-oil valve or who presses the button to manually activate the relay to close the automatic hot oil valve. Training is required.		
5.	Other Safeguard	1,00E+00	A button, connected to a SIS relay, can be pushed in the control room to manually override the hot-oil valve under existing SIS and close that valve. Training required.		

Lukitusdokumentti

Kuvassa 1 esitetään esimerkkipiirin lukitukset.

		Numero P4-3907	
	Pvm 08.11.2005	Muutos 10 | | | | |	Sivu 1 (3)
Otsikko **Reaktoreiden lukitukset (SIS).**		Alue 815/816	Tunnus KX

DC-81601

AIHEUTTAJA / TOIMINTO	SW-81603/ SW-81605 hätä seis	PSA-81605 paine >HH	TZ-81601/ TZ-81659 lpt. >HH	TZ-81601/ TZ-81659 lpt. >HHH	TIS-81609 CW-paluu lpt. >HH	XSA-81625 murtolevy murtunut	XSA-81620 sekottajan kierr. < LL	Muutos
sulkee TICA-81601.A	X	X	X			X		
avaa TICA-81601.B	X	X	X			X		
sulkee XCV-816223	X	X	X			X		
sulkee XCV-816225	X	X	X		X (huom1)	X		
avaa XCV-816227	X	X	X					
sulkee XCV-81619		X		X		X		
sulkee XCV-816109		X		X		X		
sulkee XCV-81688	(Huom.2)	X		X		X		
avaa XCV-81615 (paineen ohitus)	X							
avaa XCV-81617	X							
avaa XCV-816105	X							
avaa XCV-816107	X							
avaa XCV-816117	X							
avaa XCV-816119	X							
sulkee HSV-81635	X	X						
sulkee HSV-81603	X	X						
sulkee HSV-81605	X	X						
sulkee HSV-81607	X	X						
sulkee HSV-81623 (varalla)	X	X						
sulkee HSV-81625	X	X						
sulkee HSV-81627	X	X						
sulkee XCV-81691	X	X						
sulkee XCV-81635	X	X						
sulkee FIC-81611	X	X						
sulkee XCV-816101	X	X						
sulkee XCV-816169	X	X						10
sulkee XCV-816103	X	X	X				X	
pysäyttää GA-81651	X	X	X				X	
sulkee HSV-81631	X	X						
sulkee HSV-81633	X	X						
pysäyttää GD-81601 (sekottaja)	X							

Huom.1 : TIS-81609 >HH pakko-ohjaa joka tilanteessa XCV-816225:n auki.
Huom.2 : SW-81603/-5 avaa XCV-81688:n mikäli reaktorin paine-, lpt- tai murtolevy ei ole aiheuttanut lukitusta.

Kuva 1. Reaktoreiden lukitusdokumentti [42].

Kojeluettelo: PSA-81605

Kuvassa 1 esitetään painekytkimen PSA-81605 kojeluettelo.

KOJELUETTELO NUMERO : P4-2185 LEHTI : 122
---------- MUUTOS : 2 14 26 PVM : 08.11.90

PAINEKOJEET

TUNNUSNUMERO	:	: PSA-81605
KOHDE	:	: DC-81601
	:	: -
	:	: -
P&I-KAAVIO	:	: P1-1664
SÄÄTÖ/LOGIIKKAKAAVIO	:	: L. / L. 42
PUTKI/LAITENUMERO	:	: DC-81601
PROSESSITIEDOT		
-AINE	:	: POLYESTERI
-KÄYTTÖLÄMPÖTILA (*C)	:	: 230
-KÄYTTÖP MI/NO/MA (kPa)	:	: - / 100 / 200
-TUKKIVA AINE	:	: -
-SAATTOTYYP/LÄMPÖT (*C)	:	: - / -
LÄHETIN		
-TYYPPI	:	: PAINEKYTKIN
-SIJAINTI (KOORDIN.)	:	: -
-MITTAUSELEMENTTI	:	: -
-PROSESSILIITÄNTÄ	:	: 1/4" NPT SISÄKIERRE
-LAIP.AINE/TIIV.PINTA	:	: -
-PAINEENVÄLITIN	:	: -
-MITTAUSALUE (pe kPa)	:	: -100...0...280
-VIRITYS (pe kPa)	:	: 50
-VIESTILIIT.(PNEUM.)	:	: -
-VIESTILIIT.(SÄHK.)	:	: 3/4" NPT SISÄKIERRE
-SYÖTTÖJÄNN./ULOSTULO	:	: SPDT
-MALLI	:	: V3-V504H-S1N-S2-Z1
-VALMISTAJA	:	: BETA
-HANKINTAMÄÄRITTELY	:	: KTQ02-8
AUTOMAATIOJÄRJESTELMÄ		
-OHJAAMOKOJE,TYYPPI	:	: ALDIX,SWI
-ASTEIKKO (pe kPa)	:	: -
-PIIRTO KOJEELLE	:	: -
SÄÄTÖVENIT/LIITT KOJEET	:	: L. 0 / L.
HÄL.ASETTELU (pe kPa)	:	: L - H -
LUK.ASETTELU (pe kPa)	:	: LL - HH 50

Kuva 1. Painekytkimen PSA-81605 kojeluettelo [43].

Kojeluettelo: TICA-81601

Kuvassa 1 esitetään lämpötilamittarin TICA-81601 kojeluettelo.

KOJELUETTELO INSTRUMENT SCHEDULE	Numero	P4-2185
	Muutos Rev. 36	Lehti 51
	Alue 816	Tunnus KX
Pvm 24.10.2005	Laitenumero	

Otsikko	
LÄMPÖTILAKOJEET	
Tunnusnumero	TICA-81601
Kohde	DC-81601 LÄMPÖTILA
PI-kaavio	P1-1664
Putkilinjan numero	
PROSESSITIEDOT :	
Aine	POLYESTERI
Virtausmäärä kg/s	
Käyttöpaine kPa	0-200
Käyttölämpötila °C mi/no/ma	-/170/230
NESTE: tiheys 15°C/käyttöl.	
viskositeetti (KIN)	
KAASU: moolimassa kg/kmol	
kokoonpurist.kerroin	
ANTURI/LÄHETIN:	
Tyyppi	2xPT100 / 1xExi-LÄHETIN
Kaksoisanturi kojeelle	TZ-81601
Prosessiliitäntä	DN40 PN25 ◄
Syöttöjännite	24VDC
Viritys	/ 0-300°C
Lähtöviesti	4-20mA/RTD
Malli	2xWT-BH-12-DAN-405/270-4J-KLA / 1xPR5331B3B
Valmistaja	SKS/PRelectronics
Hankintamäärittely	816-600, 816-634 ◄
TAULUKOJE :	
Tyyppi	ALCONT
Sijainti	
Syöttöjännite	
Malli	
Valmistaja	
Hankintamäärittely	
MUUT KOJEET :	
Paikallisosoitinkoje	Lehti
Säätöventtiili	Lehti: 301
Säätöyksikkö	Lehti
Hälytysasettelu °C	L/H=
Lukitusasettelu °C	HH/HHH= 230 / 240
Huomautuksia	Lähetin erill.kotelossa TZ-81601: Valm. : PRelectronics Malli: PR5111B2 HM. : 816-602

F	Muutos Rev. Muut. TICA-81601 33/24.10.2005	Täydennetty TICA-81601 36/16.06.2006		

Kuva 1. Lämpötilamittarin TICA-81601 kojeluettelo [44].

Kojeluettelo: TZ-81659

Kuvassa 1 esitetään lämpötilakytkimenTZ-81659 kojeluettelo.

KOJELUETTELO INSTRUMENT SCHEDULE		Numero	P4-2185
		Muutos Rev. 45	Lehti 68
		Alue 816	Tunnus KX
Pvm 30.11.2004		Laitenumero	

Otsikko

LÄMPÖTILAKOJEET		
Tunnusnumero		TIZ-81659
Kohde		DC-81601 LÄMPÖTILA
PI-kaavio		P1-1664
Putkilinjan numero		
PROSESSITIEDOT :		
Aine		POLYESTERI
Virtausmäärä kg/s		
Käyttöpaine kPa		0-200
Käyttölämpötila MI/NO/MA °C		-/170/230
NESTE: tiheys 15°C/käyttöl.		
viskositeetti (KIN)		
KAASU: moolimassa kg/kmol		
kokoonpurist.kerroin		
ANTURI:		
Tyyppi		2xPT100 / 1xExi-LÄHETIN
Prosessiliitäntä		TZ-81659
Liitännät (pneum/sähk)		DN40 PN25
Syöttöjännite		24VDC
Viritys		0-300°C
Lähtöviesti		4-20mA/RTD
Malli		2xWT-BH-12-DAN-G½"-405/ 270-4J-KLA / 1xPR5331B3B
Valmistaja		SKS/PRelectronics
Hankintamäärittely		816-633, 816-634
TAULUKOJE :		
Tyyppi		ALCONT
Asteikko °C		0...300
Syöttöjännite		
Malli		
Valmistaja		ALTIM CONTROL
Hankintamäärittely		KTQ02-1
MUUT KOJEET :		
Paikallisosoitinkoje	Lehti	Lehti
Säätöventtiili	Lehti	Lehti:
Säätöyksikkö	Lehti	Lehti
Hälytysasettelu °C	L/H=	L/H=
Lukitusasettelu °C	LL/HH=	HH/HHH= 230 / 240
Huomautuksia		Lähetin erill.kotelossa TZ-81659: Valm. : PRelectronics Malli: PR5111B2 HM. : 816-635

F Muutos Rev. Lisätty lehti 30/30.11.2004	Lis. TIZ-81659 36/16.06.2006		

Kuva 1. Lämpötilakytkimen TZ-81659 kojeluettelo [45].

Kojeluettelo: XCV-816103

Kuvassa 1 esitetään venttiilin XCV-816103 kojeluettelo.

KOJELUETTELO
INSTRUMENT SCHEDULE

Numero No. P4-2185	
Muutos Rev. 37	Lehti Sheet 651
Alue Area 816	Tunnus KX
Laitenumero Equipment	

Pvm
31.10.2006

Otsikko

XCV-VENTTIILIT

Tunnusnumero	XCV-816103	
Kohde	ANNOSTELUN SULKUVENTTIILI	
PI-kaavio	P1-1664	
Putkilinjan numero	25-P-816677-A316/25	
PROSESSITIEDOT :		
Aine		
Virtausmäärä kg/s		
Paine ennen venttiiliä kPa		
Paine-ero kPa		
Käyttölämpötila °C	60	
Moolimassa kg/kmol		
Tiheys 15C/ käyt.läm.tila kg/m3	/1310	
Viskositeetti mm2/s	1,6 cP	
Kriittinen paine		
Höyrynpaine käyttölämpöt.		
Höyryst.osa (kg/s) / moolimassa		
Laskettu/ valittu Cv		
PESA :		
Tyyppi ja mallinumero	TULPPA	
Koko	DN25	
Liitännät	DN25 PN16	
Laipan tiivistepinta		
Materiaali	DUPLEX (1.4462)	
SISÄOSAT:		
Tyyppi tulpat/istukat	TULPPA	
Koko	DN25	
Materiaali	DUPLEX (1.4462)	
Valmistajan Cv		
Venttiilin malli	120 FS	
Toimilaitteen tyyppi	PNEUM./ 1-TOIMINEN	
Toimilaitteen malli	ES 200/5	
Jousen toiminta	SULKEE	
ASENNOITIN:		
Tyyppi		
Malli		
Tuloviesti		
Lähtöviesti		
Valmistaja	3Z / EL-O-MATIC	
Hankintamäärittely	816-670	

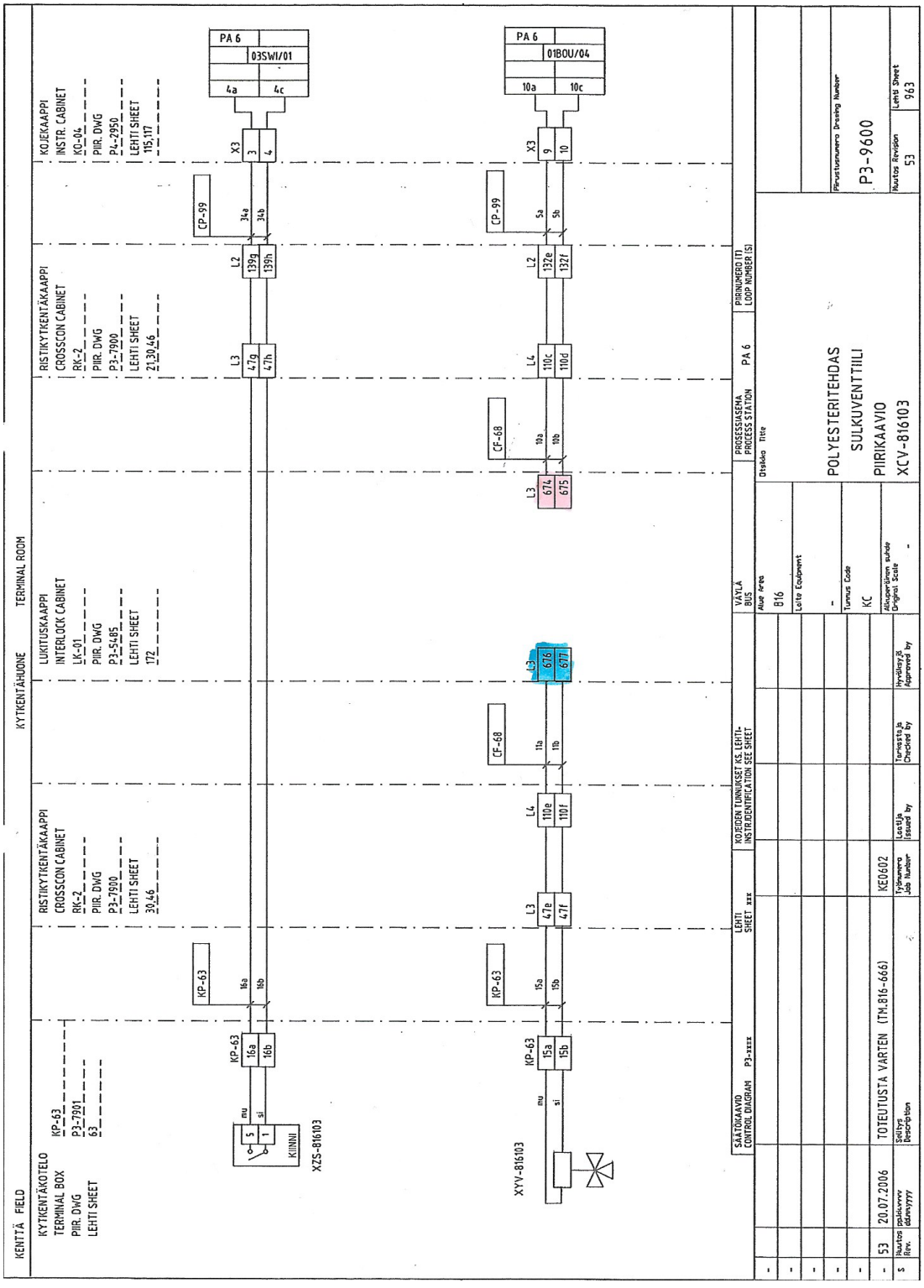
Huomautuksia ja lisätietoja

F	**Muutos Rev.:** Lisätty lehti 37/31.10.2006/		

Kuva 1. Venttiilin XCV-816103 kojeluettelo [46].

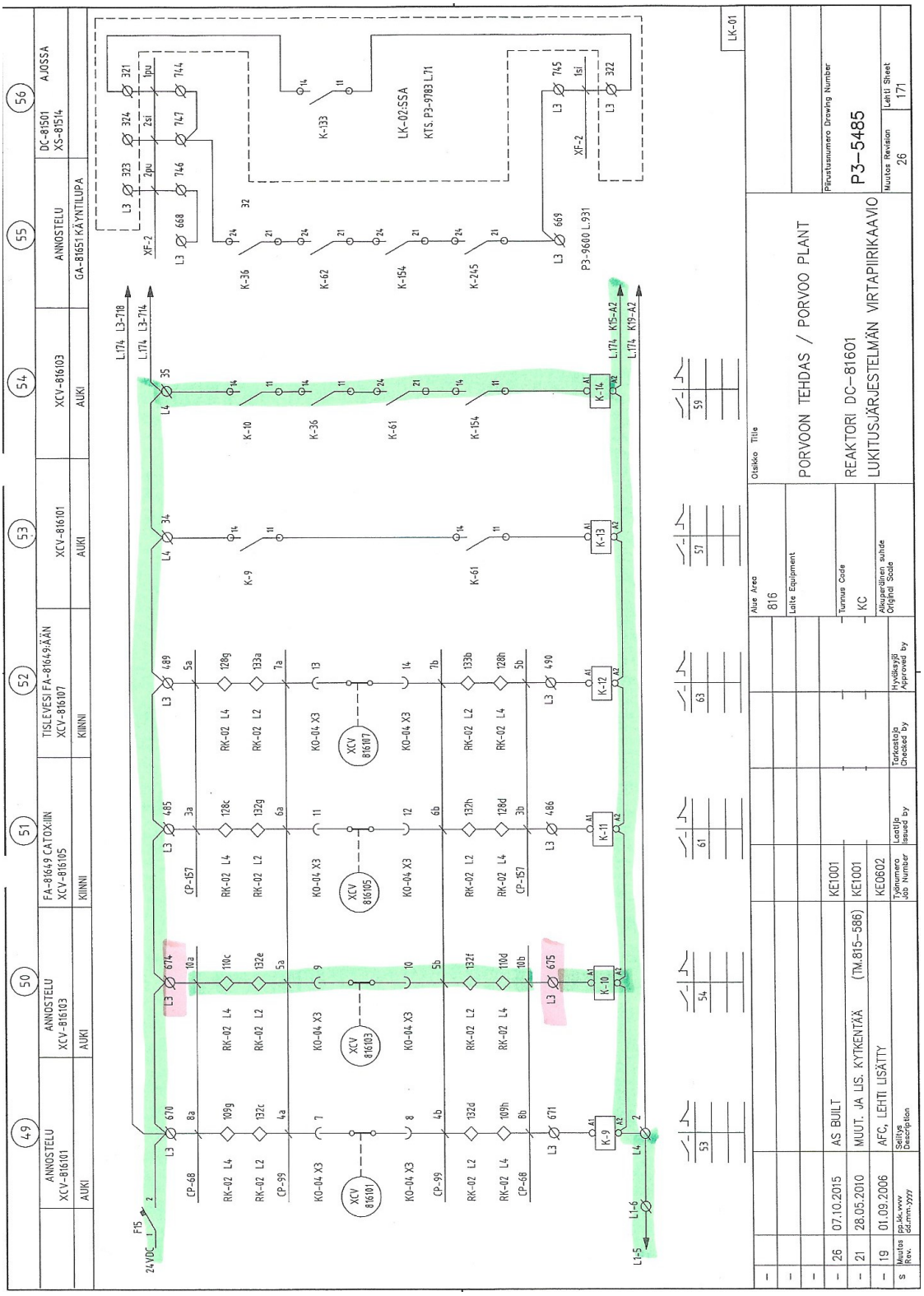
Esimerkkipiirin lukitusjärjestelmän virtapiirikaaviot

Kuvassa 1 esitetään venttiilin XCV-816013 piirikaavio.



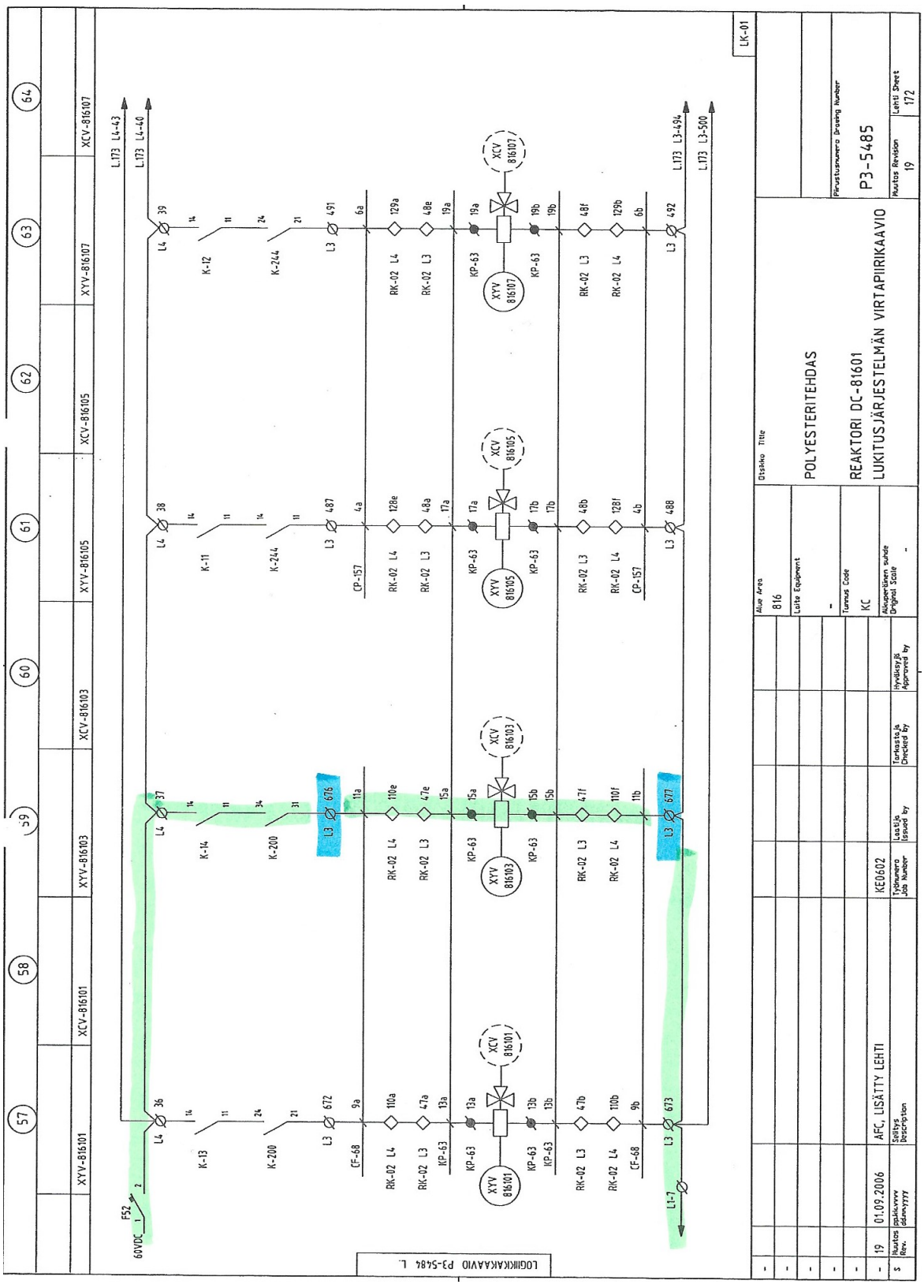
Kuva 1. Venttiilin XCV-816103 piirikaavio [47].

Kuvassa 2 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 1/8. Vihreä korostus osoittaa esimerkkipiiriin kuuluvan osan virtapiirikaaviossa.



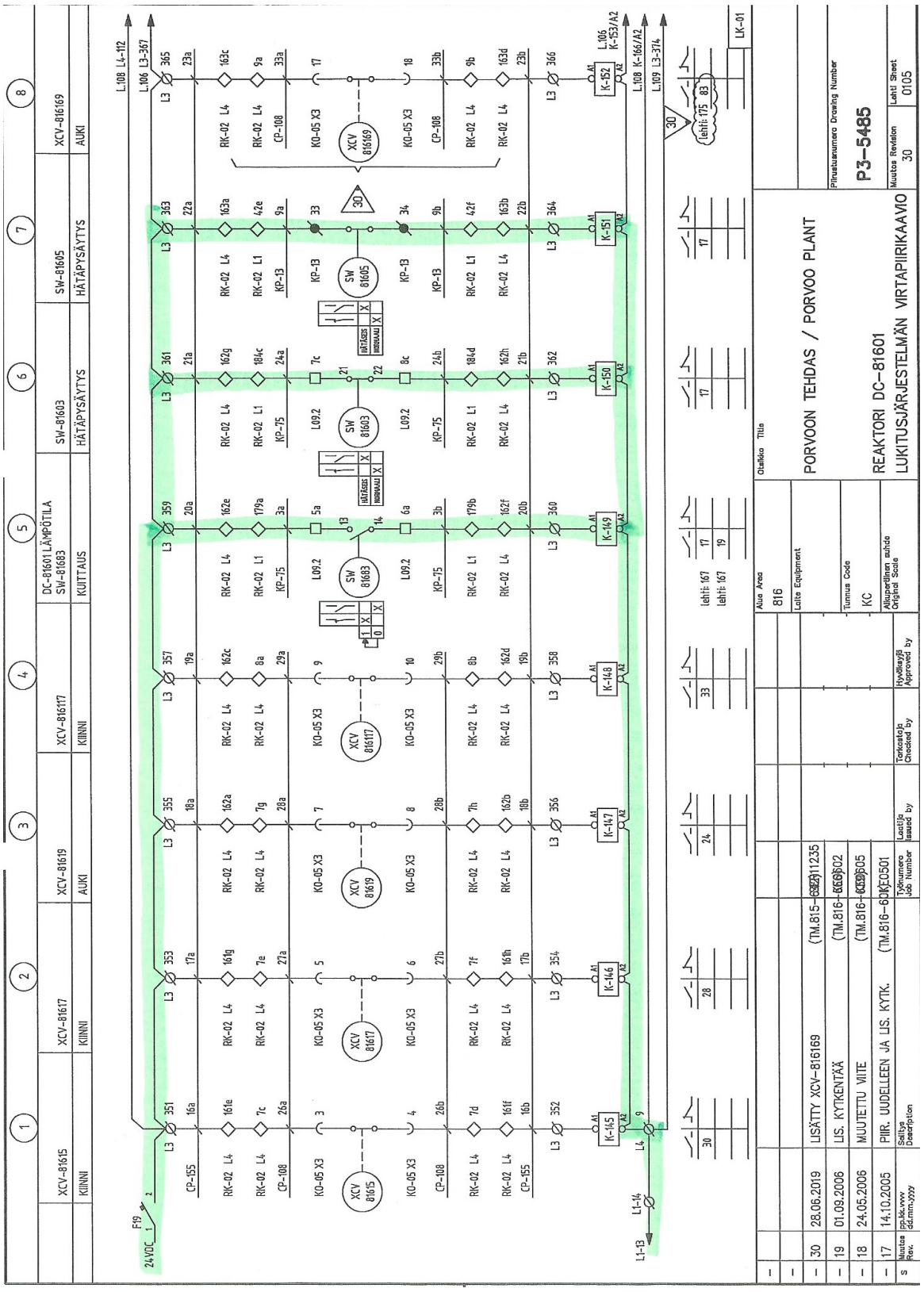
Kuva 2. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 1/8 [48].

Kuvassa 3 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 2/8.



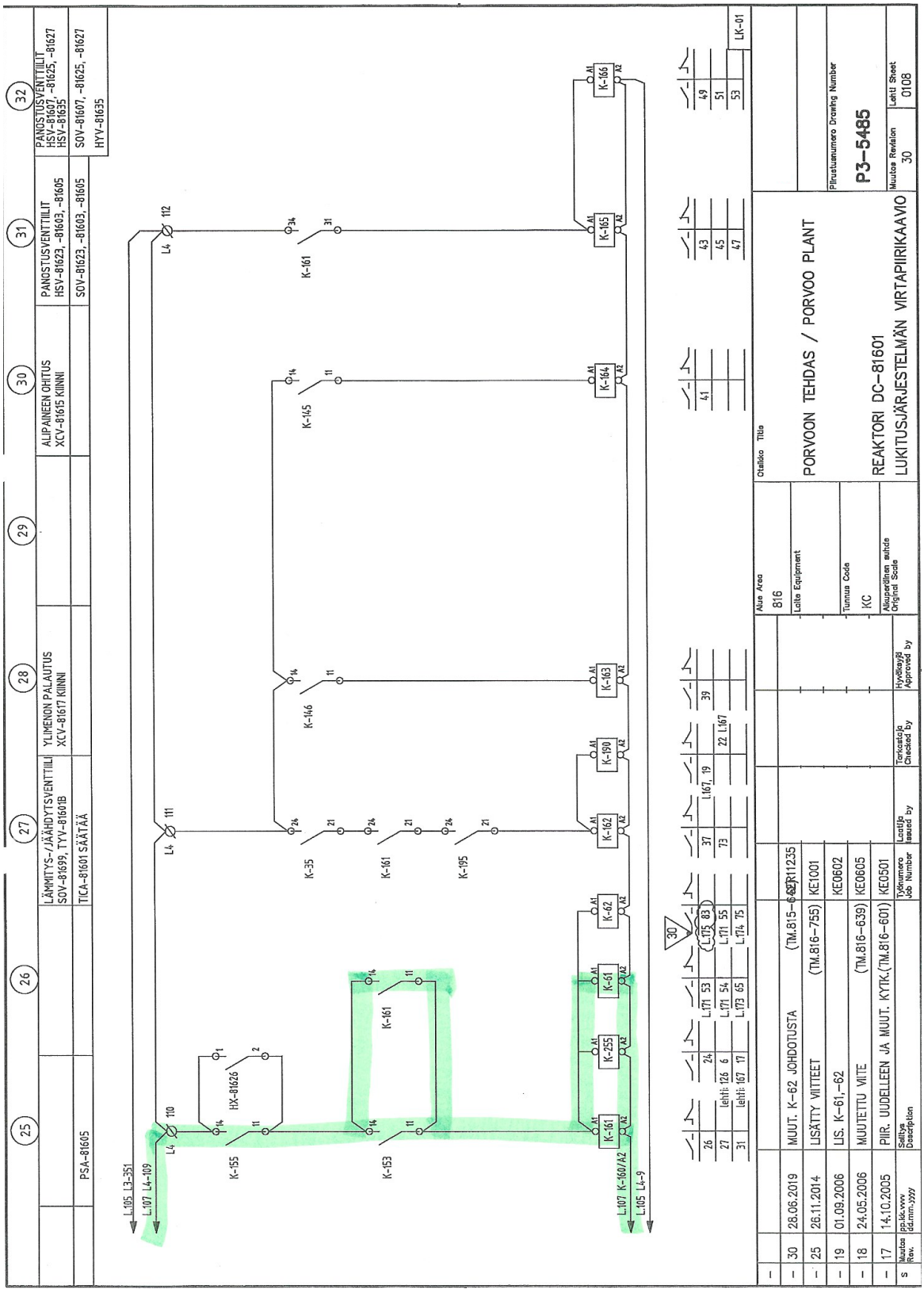
Kuva 3. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 2/8 [49].

Kuvassa 4 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 3/8.



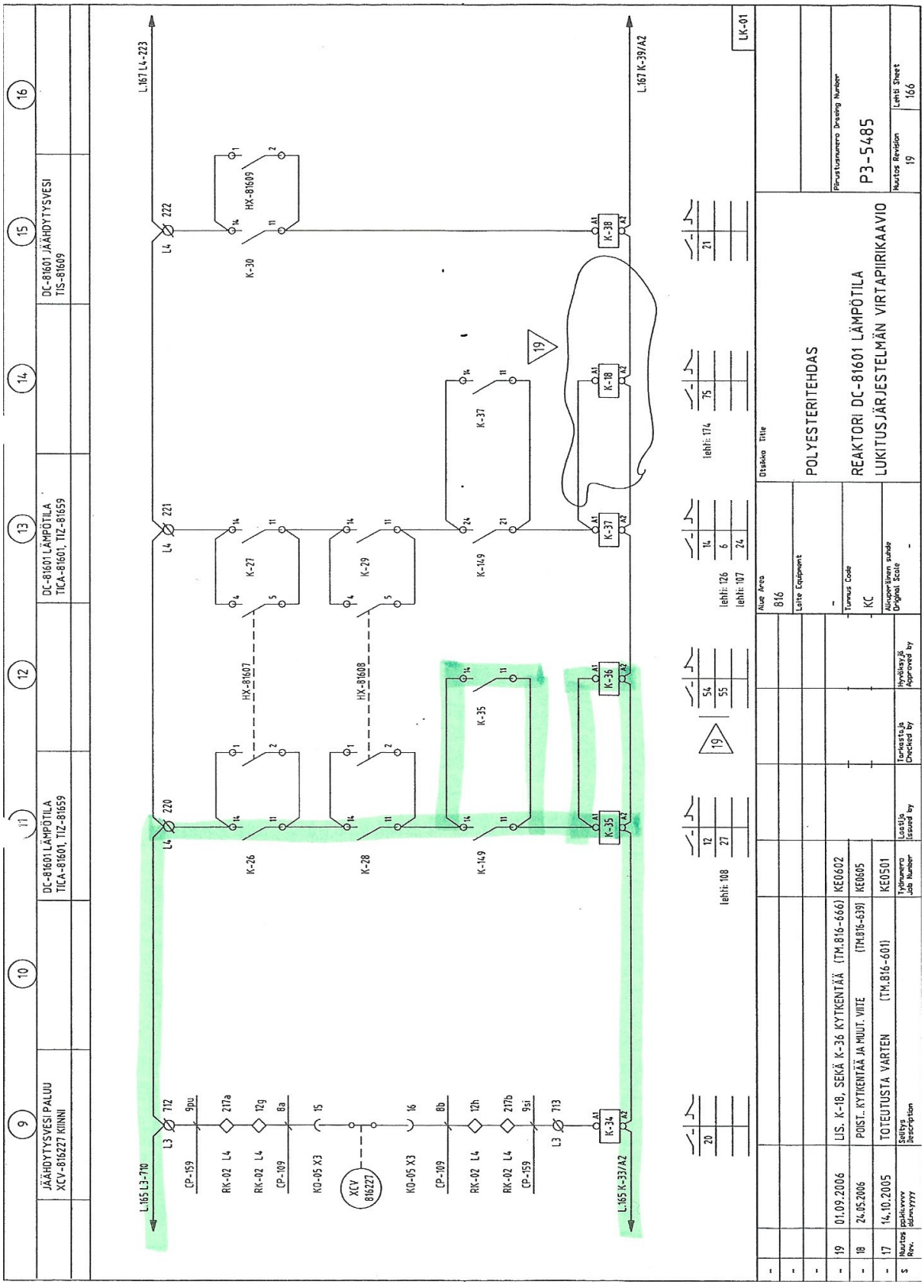
Kuva 4. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 3/8 [50].

Kuvassa 5 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 4/8.



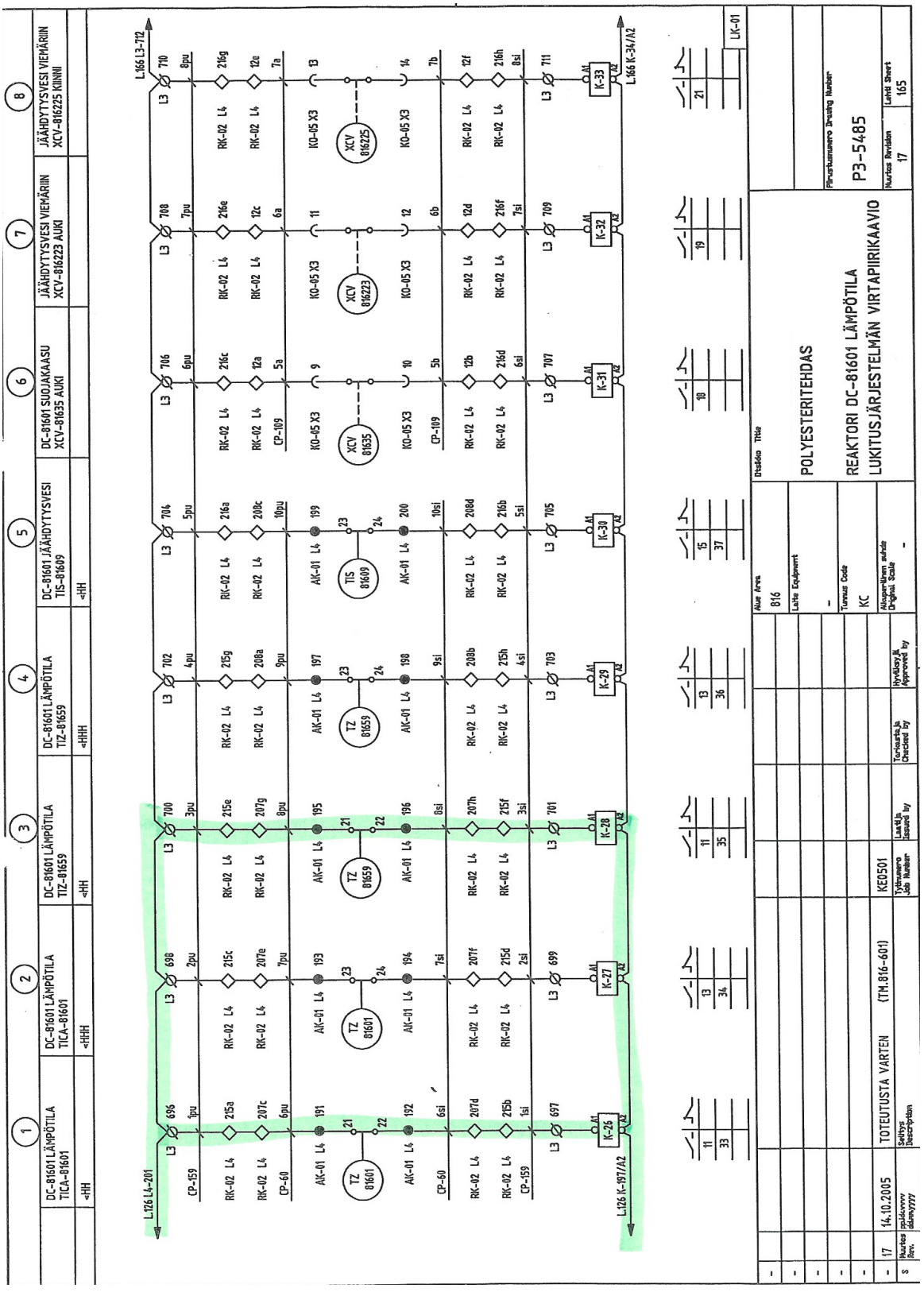
Kuva 5. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 4/8 [51].

Kuvassa 6 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 5/8.



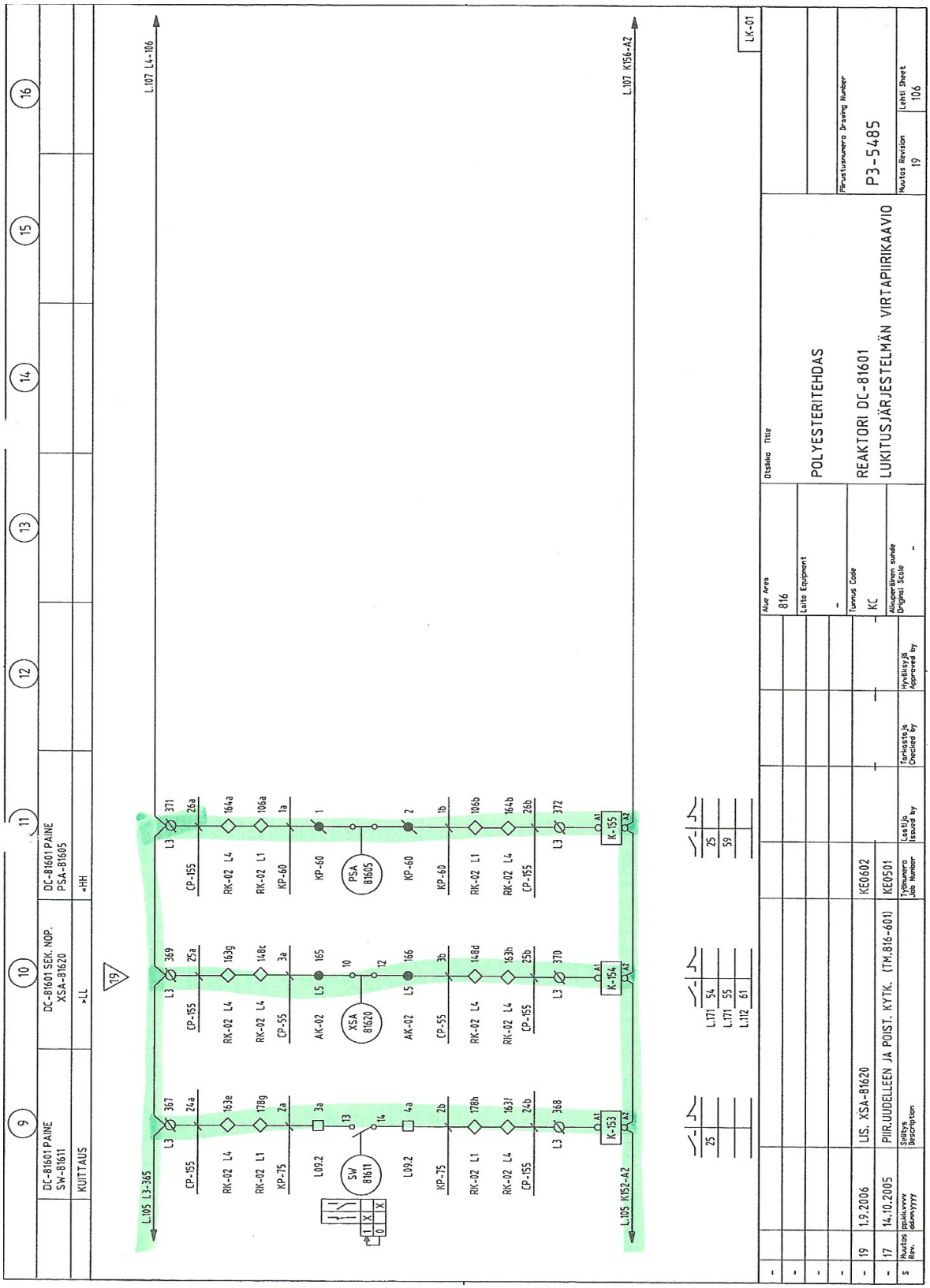
Kuva 6. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 5/8 [52].

Kuvassa 7 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 6/8.



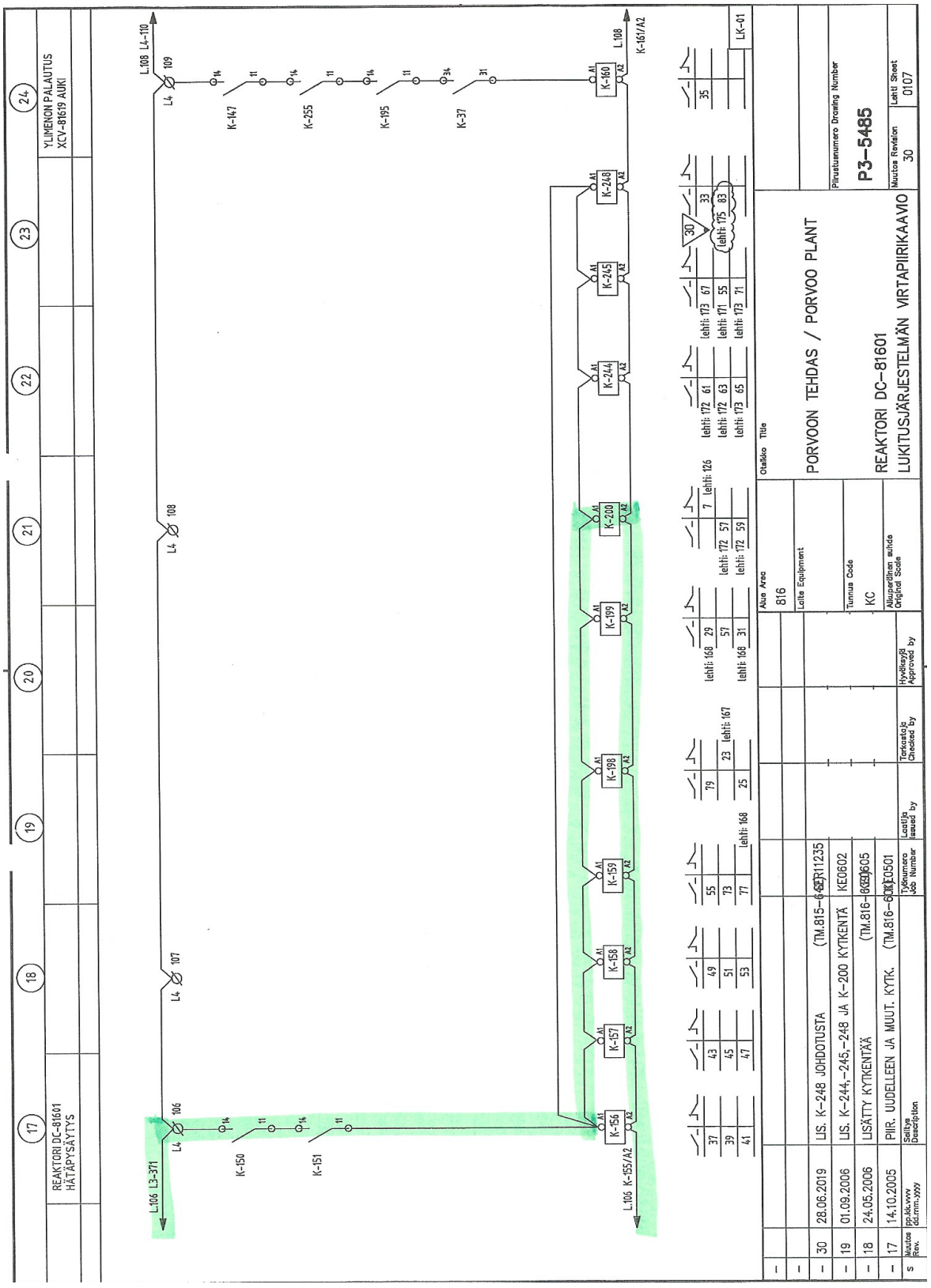
Kuva 7. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 6/8 [53].

Kuvassa 8 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 7/8.



Kuva 8. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 7/8 [54].

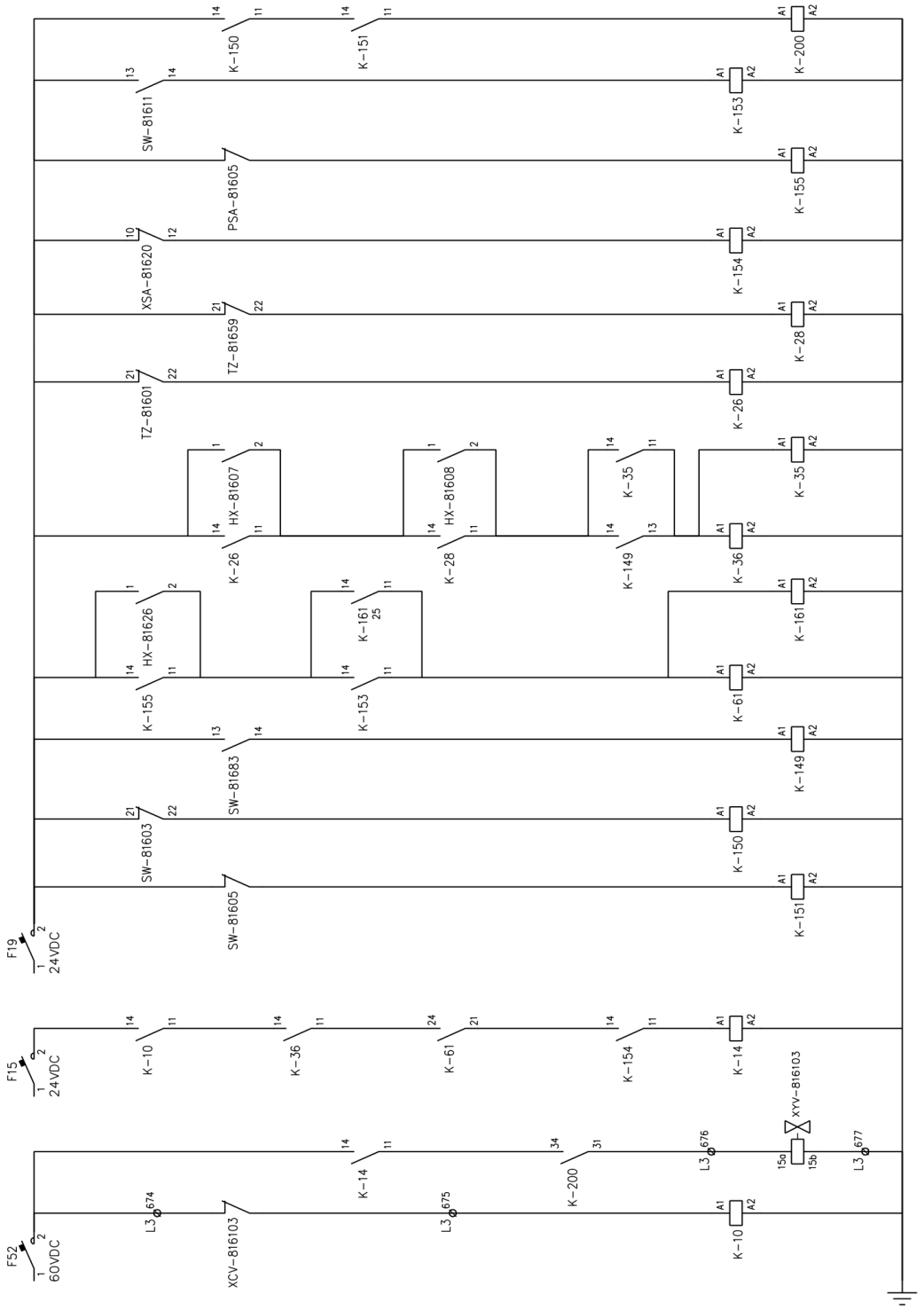
Kuvassa 9 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 8/8.



Kuva 9. Esimerkkipiirin lukitusjärjestelmän virtapiirikaavio 8/8 [55].

Yksinkertaistus liitteestä 7

Kuvassa 1 esitetään esimerkkipiirin lukitusjärjestelmän virtapiirikaavion yksinkertaistettu versio.



Kuva 1. Esimerkkipiirin yksinkertaistettu virtapiirikaavio.