TUKES OPAS

TURVA-AUTOMAATIO PROSESSITEOLLISUUDESSA

TURVATEKNIIKAN KESKUS

Turva-automaatio prosessiteollisuudessa

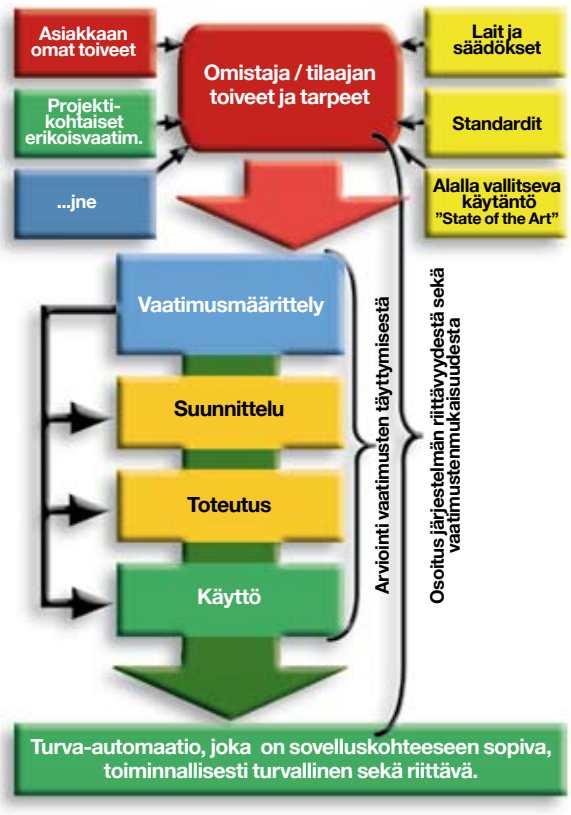
Prosessilaitosten ja prosessien riskejä voidaan vähentää monin tavoin - ensisijaisesti hyvällä prosessi- ja laitossuunnittelulla. Yhtenä riskinvähennyskeinona toimii turva-automaatiojärjestelmä, joka on prosessin tai laitteen normaalista käyttöautomaatiosta erillinen järjestelmä. Turva-automaatio pysäyttää prosessin ja laitteen tai ohjaa sen vakavassa häiriö- tai vaaratilanteessa turvalliseen tilaan. Turva-automaatio toimii, mikäli käyttöautomaatiojärjestelmä tai muu varautuminen pettää. Turva-automaatiojärjestelmä vaikuttaa merkittävästi prosessin tai laitteen turvallisuuteen. Sen virheellisestä toiminnasta tai toimimattomuudesta saattaa olla seurauksena vakavia henkilö-, ympäristö- tai omaisuusvahinkoja.

Tässä oppaassa kuvataan turva-automaatiojärjestelmään liittyviä arvioinnin ja hyväksymisen menettelyjä prosessiteollisuudessa. Menettelyjä suositellaan käytettäväksi silloin, kun on kyse prosessin tai laitteen turva-automaatiosta ja niitä sovelletaan koko turvajärjestelmään, eli esimerkiksi mittalaitteisiin, logiikkaan, releistyksiin, kaapelointeihin ja toimilaitteisiin. Menettelyjä sovelletaan uusiin prosesseihin ja käytössä olevien järjestelmien muutoksiin tai uudistuksiin.

Opas tarjoaa tietoa erityisesti yritysten tuotannosta ja turvallisuudesta vastaaville henkilöille ja vastaa kysymyksiin: Mitä pitää ottaa huomioon hankittaessa turva-automaatiojärjestelmä ja miten varmistetaan järjestelmän toiminnallinen turvallisuus. Tavoitteena on, että laitokseen valitaan riittävän tasokkaat järjestelmät, joihin voi luottaa koko laitoksen toiminta-ajan.

Joulukuu 2007

TURVATEKNIIKAN KESKUS



1. Turva-automaatio toiminnallisen turvallisuuden varmistajana

Turva-automaatio on tärkeä varautumismenetelmä prosessiteollisuuden toiminnallisen turvallisuuden varmentamisessa. Toiminnallisella turvallisuudella tarkoitetaan sitä osaa kokonaisturvallisuudesta, joka riippuu järjestelmien ja laitteiden oikeasta ja oikea-aikaisesta toiminnasta. Toiminnallinen turvallisuus on riittävää silloin, kun prosessi sekä siihen liittyvät järjestelmät on määritetty oikein, ne toimivat luotettavasti ja ennakoidusti - siten, kuin niiden on tarkoitettukin toimivan - eivätkä ne aiheuta vahinkoa tai vaaraa. Turva-automaatiojärjestelmän (TAJ) on oltava toimintansa ja rakenteensa puolesta kyseiseen käyttötarkoitukseen ja olosuhteisiin sopiva.

Turva-automaatiojärjestelmille asetettuja vaatimuksia ovat:

- Turva-automaatiojärjestelmän tulee olla käyttöautomaatiosta riippumaton.
- Järjestelmän suunnittelussa on otettava huomioon prosessin luonteen ja vaarallisuuden kannalta riittävä luotettavuus.
- Järjestelmän ja siihen liittyvien laitteiden turvallisuus, luotettavuus ja soveltuvuus kohteeseen on kyettävä osoittamaan sekä arvioimaan.
- Ensisijaisesti on käytettävä turvallisuuskäyttöön tyyppihyväksyttyjä laitteita.
- Järjestelmän on toimittava riittävän suurella todennäköisyydellä virheettömästi myös sellaisessa vaaratilanteessa, joka voi sattua vain kerran laitoksen koko elinkaaren aikana.
- Järjestelmä ei saa aiheuttaa prosessia ja turvallisuutta vaarantavia tarpeettomia pysäytyksiä tai alasajoja.
- Laitteiden tulee olla mahdollisimman huoltovapaita ja helposti huollettavia sekä koestettavia.
- Prosessissa tulee olla järjestelmästä riippumaton käsin pysäytyksen mahdollisuus.
- Häiriötilanteessa toimilaitteet jäävät tai siirtyvät ennalta määritettyyn turvalliseen tilaan.

Prosessien riskit ja riskien vähennys

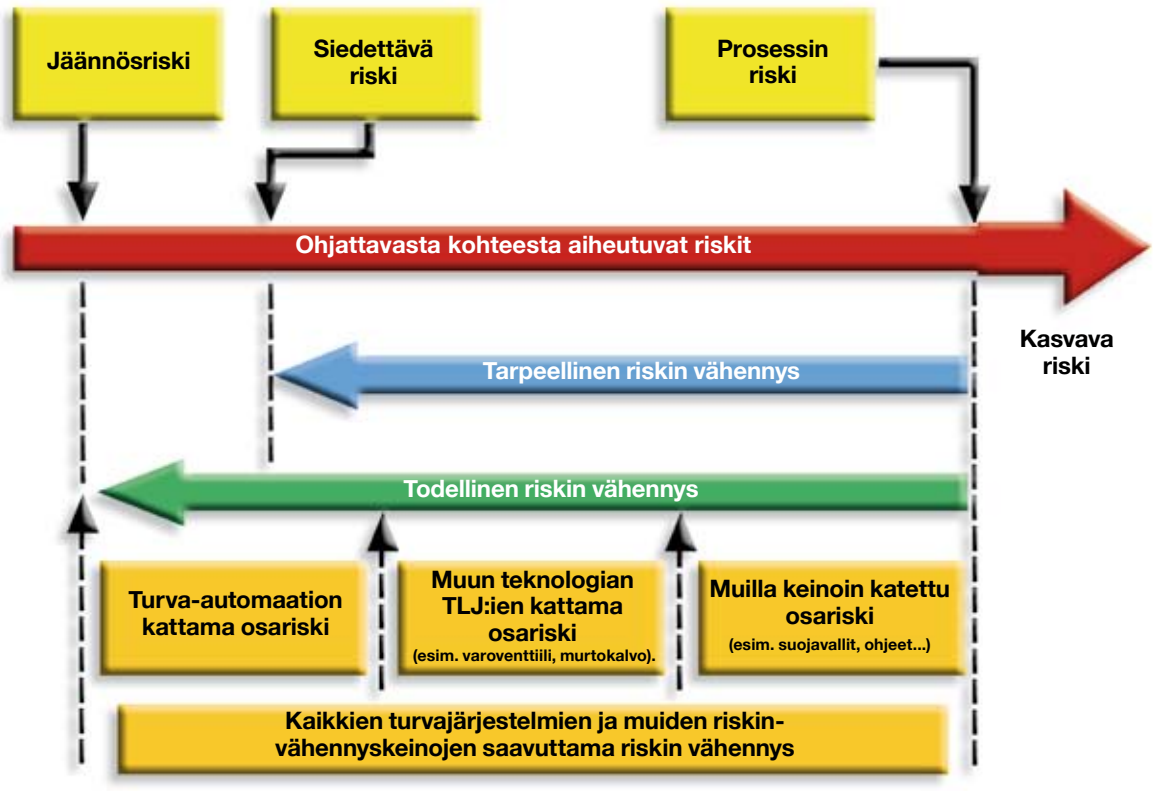
Prosessilaitosten tai vaarallisten laitteiden suunnittelun yleinen periaate on, että riskit arvioidaan ja varautuminen tehdään riskin edellyttämällä tasolla. Mitä vaarallisempi on prosessi, sitä enemmän luotettavutta on vaadittava riskinvähennykseltä (esim. turva-automaatiolta) ja järjestelmien riittävyyden osoittamiselta. Toiminnallisen turvallisuuden lähtökohtana on ohjattavan kohteen riskin arviointi ja vaatimusten määrittely, joiden perusteella määritellään varautumiselle tarvittava turvallisuuden eheyden taso (TET). Järjestelmän suunnittelu ja toteutus tähtäävät tämän vaaditun turvallisuuden eheyden tason saavuttamiseen.

Jos turvatarkasteluissa esimerkiksi todetaan, että lämpötilan noususta voi olla seurauksena vakava onnettomuus (eksotermisiä reaktioita, paineen nousu jne.) on harkittava, tarvitaanko perusautomaation lisäksi erillinen turva-automaatiojärjestelmä, ja kuinka luotettava kyseisen riskin vähennyksen tulisi olla. Oleellista on tarkastella, miten riskien poiston kannalta kriittisten laitteiden tai järjestelmien luotettavuus on varmistettu ja miten kyetään osoittamaan niiden riittävyys.

Turva-automaatio on aina vain osa prosessin kokonaisriskien vähentämistä. Tapauskohtaisesti on aina tarkasteltava ja määriteltävä, kuinka paljon riskinvähennystä turva-automaatiolta edellytetään.

Kuvassa 2 esitetään riskinvähennyksen yleiset periaatteet.

- Prosessin riski tarkoittaa riskiä, joka voi aiheutua joko itse prosessista tai sen vuorovaikutuksesta ohjausjärjestelmänsä kanssa, mukaan lukien operaattorien toimet.
- Siedettävä riski on määritelty riskinä, joka hyväksytään tietyssä yhteydessä yhteiskunnan senhetkisten arvojen mukaan. Se saattaa vaihdella eri toimialoilla, maissa ja yrityksissä.
- Jäännösriskin tulee olla pienempi kuin siedettävä riski. Tähän päästään erilaisilla riskinvähennyskeinoilla.



Kuva 2. Riskin vähennys: yleiset periaatteet (IEC 61508)

2. Yleiset turvallisuusvaatimukset prosessilaitosten turva-automaatiojärjestelmille

2.1 Turva-automaatiojärjestelmän säädösvaatimuksia

Painelaite- ja kemikaaliturvallisuussäädösten peruslähtökohtana on, että prosessilaitoksista tai niihin liittyvistä laitteista ja järjestelmistä ei saa aiheutua henkilö-, ympäristö- tai omaisuusvahinkoja odotettavissa olevan elinkaaren aikana. Säädöksissä esitetään olennaisia vaatimuksia turvallisuuteen liittyvien laitteiden ja järjestelmien toiminnalliselle turvallisuudelle. Säädöksissä esitetään vaatimuksia mm. turva-automaatiojärjestelmien tilaajalle/toiminnanharjoittajalle (omistaja/haltija), valmistajalle/toimittajalle sekä tarkastuslaitokselle ja viranomaiselle. Vaatimukset koskevat sekä uusia että käytössä olevia laitteita ja niihin tehtäviä muutoksia.

Toiminnanharjoittajan on osoitettava laitosta käyttöönotettaessa sekä määräajoin, että järjestelmä on varustettu riittävillä käyttöturvallisuuteen vaikuttavilla laitteilla ja järjestelmillä, jotka toimivat asianmukaisesti. Viranomaiset ja tarkastuslaitokset tarkastelevat toteutettujen järjestelmien asianmukaisuutta laitoksiin tekemissään valvonta- ja määräaikaistarkastuksissa.

Kemikaalisäädösten mukaan toiminnanharjoittajan on osoitettava, että kemikaalien käsittely on turvallista, ja onnettomuuksiin varautuminen sekä valitut turvajärjestelmät ovat riskeihin suhteutettuna riittäviä. Kemikaalisäädöksissä ei vaadita tietyn standardin tai ohjeen käyttöä, joten turva-automaatiota koskevat valinnat ja vaatimustenmukaisuuden osoittaminen jäävät toiminnanharjoittajan tehtäväksi. Painelaitesäädösten mukaisilla menettelyillä voidaan osoittaa myös kemikaalilainsäädännön piiriin kuuluvan turva-automaatiojärjestelmän vaatimustenmukaisuus, kunhan otetaan huomioon prosessista ja kemikaaleista aiheutuvat riskit.

Painelaitesäädöksissä turva-automaatio liittyy ennen kaikkea laitekokonaisuuksien arviointeihin ja määräaikaistarkastuksiin. Säädöksissä kuvataan menettelyt, joilla voidaan osoittaa varo- ja suojalaitteina käytettävien järjestelmien vaatimustenmukaisuus.

Järjestelmien toteutuksissa tulee ottaa huomioon myös muut kohdetta koskevat työ- ja tuoteturvallisuussäädökset, esim. kone-, pienjännite- ja EMC-direktiivien vaatimukset.

Toteutuksen suunnitelmat ja menettelyjen asianmukaisuus tulee hyväksyttää tai esittää laitoksen lupakäsittelyjen ja tarkastusten yhteydessä. Yhteydenpito kaikkiin asianomaisiin tahoihin on aloitettava riittävän ajoissa, jotta toteutukseen voidaan vaikuttaa.

2.2 Turva-automaatiojärjestelmän standardeja ja ohjeita

Henkilöturvallisuuteen liittyvien sähköteknisten ohjausjärjestelmien turvallisuuden määrittelylle on laadittu yleis- eli kattostandardi IEC 61508. *(Sähköisten/ elektronisten/ ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus)*. Kattostandardi sisältää toiminnallisen turvallisuuden varmistamiseen liittyviä vaatimuksia ja sovelluksien yleisiä ohjeita järjestelmien kaikille elinkaaritoimille. CENELEC on vahvistanut sen eurooppalaiseksi standardiksi (EN 61508). Kattostandardissa esitettävät menettelyt ovat usein riittäviä myös direktiivien olennaisten turvallisuusvaatimusten täyttämisessä ja niitä voidaan pitää alalla vallitsevina hyvinä käytäntöinä.

Toimiala- tai järjestelmäkohtaisia sovellusstandardeja on olemassa mm. prosessiteollisuudelle (IEC 61511) ja koneen turvallisuuteen liittyville ohjausjärjestelmille (IEC 62061). Näiden kaikkien standardien lähtökohtana on elinkaariajattelu, laatujärjestelmän mukainen suunnitelmallinen toiminta ja turvallisuuteen liittyvien järjestelmien toiminnallisen turvallisuuden osoittaminen. Kohteen, kuten prosessin, riskien perusteella määritetään toiminnalliseen turvallisuuteen liittyvä vaatimustaso, eli kuinka suurella varmuudella järjestelmän tulee toimia. Vaatimustasoon perustuen valitaan niin tekniset kuin ei-tekniset ratkaisut. Ei-tekniset ratkaisut liittyvät esimerkiksi laadunhallintaan, pätevyyksiin, suunnitteluun, asennukseen, käyttöön ja kunnossapitoon.

Turvatoimintojen suunnittelussa ja toteuttamisessa sähköisellä, elektronisella ja ohjelmoitavalla tekniikalla suositellaan noudatettavan kattostandardin tai sovellusstandardien vaatimuksia. Standardien noudattaminen on vapaaehtoista – ne ovat kuitenkin yksi tapa osoittaa järjestelmien soveltuvuus tarkoitettuun tehtäväänsä. Tukes suosittelee edellä mainittujen standardien peruspe-

riaatteiden käyttöä yhdessä sovelluskohtaisten teknisten ohjeiden kanssa (esim. KLTK-ohjeet ja muut toimialakohtaiset ohjeet). Valmistajat voivat valita myös muun menettelyn, joka täyttää säädösten vaatimukset.

Mitä riskialttiimpi prosessi on, sitä luotettavampaa on oltava riskinvähennykseen käytetyn tekniikan. Jokaiselle erilliselle turvatoiminnolle on määritettävä vaadittava turvallisuuden eheystaso (TET), joka vastaa turvatoiminnon vikaantumisen todennäköisyyttä. Turvallisuuden eheys tarkoittaa sitä, että turvatoiminto toteuttaa hyväksyttävästi vaadittavat tehtävät kaikissa määritellyissä olosuhteissa ja määritellyn ajan. Mitä korkeampi on turvallisuuden eheystaso, sitä todennäköisempää on, että kyseinen turvatoiminto toimii vaaratilanteessa oikein. Turvallisuuden eheyden eri tasoille on annettu kattostandardissa menetelmätai tekniikkavaatimuksia, jotka ovat sitä vaativampia, mitä korkeampi on taso. TET vaikuttaa siihen, millaisia laiteteknisiä vaatimuksia annetaan järjestelmän rakenteelle (arkkitehtuurirakenne ja vikasietoisuus) ja toimintatodennäköisyydelle ja millaisia arviointivaatimuksia asetetaan järjestelmän riittävyyden sekä vaatimustenmukaisuuden osoittamiselle.

2.3 Turva-automaatiojärjestelmän toteutusvaiheet

Laitteista tai järjestelmistä ei saa aiheutua vahinkoa tai vaaraa koko niiden suunnitellun elinkaaren aikana, ja siten turva-automaation toteuttamisessa keskeisimmät osa-alueet ovat toiminnallisen turvallisuuden järjestelmällinen hallinta sekä elinkaariajattelun noudattaminen. Jotta turvallisuutta käsiteltäisiin järjestelmällisesti, on standardissa IEC 61508 otettu käyttöön turvallisuuden elinkaari, jossa projekti on jaettu vaiheisiin määrittelystä järjestelmän poistoon saakka. Vaiheille on määritelty laajuus eli puitteet, tavoitteet, vaatimukset sekä tulo- ja lähtötiedot.

Toiminnallisen turvallisuuden varmistamisessa on tavoitteena, että tekniset järjestelmät toimivat tarkoitetulla tavalla niin tavanomaisessa käytössä kuin myös poikkeustilanteissa. Kaikkien näiden toimintojen hallintaan tarvitaan kattava turvallisuuden hallintajärjestelmä, jossa määritetään yleiset organisatoriset ja tekniset menetelmät turvallisuuden saavuttamiseksi ja sen ylläpitämiseksi. Turvallisuuden elinkaaren rinnalla kulkee myös arviointi, jossa muodostetaan riippumaton käsitys tavoitellun toiminnallisen turvallisuuden saavuttamisesta. Turva-automaatiojärjestelmän riittävyys tunnistettuihin riskeihin nähden on kyettävä osoittamaan ennen käyttöönottoa sekä määräajoin käytön aikana.

Toiminnallisen turvallisuuden varmistaminen tulee tehdä järjestelmän kaikille elinkaaren vaiheille lähtien määrittelystä, suunnittelusta, toteutuksesta ja käyttöönotosta edeten järjestelmän käyttöön, kunnossapitoon ja järjestelmän muutoksiin. Toteutuksen riittävyys suunniteltuun tehtävään nähden tulee osoittaa vaiheittain, jotta lopputulos on sovelluskohtaisesti kelvollinen ja täyttää sille asetetut vaatimukset.

Seuraavassa taulukossa kuvataan turva-automaation turvallisuuden eri elinkaaren vaiheita ja niihin sisältyviä toimenpiteitä. Kuvausta voi soveltaa kaikkiin laitoksen prosesseihin, laitteistoihin ja yksittäisiin laitteisiin.

Elinkaarivaihe	Kuvaus
Vaatimus-määrittely	Vaatimusmäärittelyn tärkein tehtävä on varmistaa, että prosessin toimintaan liittyvät ja toimialaa koskevat vaatimukset (esim. noudatettavat säädökset ja standardit) sekä riskit on otettu riittävän hyvin huomioon. Turva-automaatiota koskevassa määrittelyssä on oltava turvatoimintojen toteuttamiseen ja luotettavuuteen liittyvät tiedot. Lähtökohtana on laitteiden tai prosessin vaarojen tunnistus ja riskien arviointi sekä niiden perusteella tehty vaatimusmäärittely turvatoiminnoille, joilla riski voidaan pienentää hyväksyttävälle tasolle. Turva-automaation elinkaaren aikana esiintyvät, tarkoitettuun käyttöön ja ennakoitavissa olevaan väärinkäyttöön liittyvät vaarat ja riskit tunnistetaan ja analysoidaan. Riskien arvioimisen ja eheystason valinnan tekee asiantunteva ryhmä. Muista vastaavista kohteista saatavia kokemuksia kannattaa selvittää ja käyttää hyödyksi. Turvallisuusratkaisuissa tulee noudattaa seuraavia periaatteita: (1) vaarojen poistaminen ja pienentäminen (2) suojaustoimenpiteet niiden vaarojen osalta, joita ei voida poistaa ja (3) tiedottaminen käyttäjälle jäljelle jäävistä vaaroista. Turva-automaatiojärjestelmän ja siihen liittyvien laitteiden ja laitteistojen hankinnassa, arvioinnissa ja vaatimustenmukaisuuden osoittamisessa käytettävät periaatteet, käytännöt ja menettelyt määritellään turvajärjestelmien toteuttamiseen liittyvään turvallisuussuunnitelmaan. Todentamiseen sovellettavat menettelyt (esim. painelaitemoduulit) ja osapuolet tulee määritellä. Valvontaviranomaiselle (kemikaalit) tehdään lupahakemus tai ilmoitus, ja/tai ollaan muuten yhteydessä riittävän aikaisessa vaiheessa valvontaviranomaiseen tai tarkastuslaitokseen. Arvioidaan määrittelyn riittävyys ja todetaan, onko edellytykset projektin toteuttamiselle ja voidaanko suunnittelua jatkaa.
Suunnittelu	Turva-automaatio on suunniteltava ottaen huomioon määrittelyvaiheen vaatimukset. Suunnittelussa on otettava huomioon vaadittu riskien vähennysvaatimus, ja kaikki muut sellaiset tärkeät tekijät, joiden ansiosta on mahdollista varmistaa laitoksen turvallisuus koko käyttöiän ajan. Toiminnallisen turvallisuuden saavuttamiseen liittyvät menettelytavat ja strategiat määritetään turvallisuussuunnitelmassa. Turva-automaatiolta edellytetään, että sen tulee pysäyttää prosessi tai saattaa se muuten turvalliseen tilaan vakavan häiriön sattuessa, eikä se saa aiheuttaa turvallisuuden kannalta tarpeettomia pysäytyksiä. Turva-automaation on oltava siten suunniteltu ja valmistettu, että se on luotettava, soveltuu suunniteltuihin käyttöolosuhteisiin, ja laitteen huoltoa sekä koestusta koskevat vaatimukset on otettu huomioon. Turvalaitteiden on oltava muista toiminnoista riippumattomia, paitsi jos muut toiminnot eivät vaaranna turvalaitteiden toimintaa. Turvalaitteiden osalta tulee noudattaa laatujärjestelmien mukaisia toimintaperiaatteita sekä asianmukaisia suunnitteluperiaatteita, jotta sopiva ja luotettava suojaus saavutetaan. Näihin periaatteisiin kuuluvat erityisesti turvallinen vikaantuminen, varmennus, erilaisuus ja itsediagnostiikka. Arvioidaan, vastaako suunnittelu määritysvaiheessa asetettuja vaatimuksia ja todetaan edellytykset projektin toteutuksen jatkamiselle.

Elinkaarivaihe	Kuvaus
Toteutus	Toteutusvaiheessa toteutetaan suunnitteluvaiheessa hyväksytyt suunnitelmat asianmukaisesti, tarkoituksenmukaisia tekniikoita ja menetelmiä käyttäen. Tavoitteena on toteuttaa turvallisuusvaatimusten määrittelyn mukaiset järjestelmät. Valmiiseen laitteeseen, laitekokonaisuuteen tai laitokseen liitetty, asianmukaisesti arvioitu turvajärjestelmä ja siihen liittyvät kenttälaitteet merkitään, ja laaditaan tarvittavat asiakirjat sekä käyttöohjeet. Arvioidaan, vastaako toteutus määrittely- ja suunnitteluvaiheessa asetettuja vaatimuksia (laitekokonaisuuden kelpoistus) ja todetaan edellytykset käyttöönottoon.
Käyttö	Käyttövaiheessa huolehditaan siitä, että järjestelmät toimivat edelleen suunnitellulla tavalla ja muutokset tehdään turvallisesti. Käyttöönotettaessa ja määräajoin on varmistettava, että häiriötilanteissa laitoksen turvallisessa tilassa pitävät laitteet ja laitteistot toimivat suunnitellulla tavalla. Tämän tulee yleensä tapahtua laitteen/järjestelmän valmistajan laatimien ohjeiden mukaisesti. Kaikille turva-automaatioon kuuluville laitteille on määriteltävä määräaikaistarkastus- tai testausväli ja menettelyt, joilla järjestelmään luotettavuus kyetään ylläpitämään. Tarkastuksen ja mahdollisten korjausten tekemiseen on nimettävä vastuuhenkilöt. Etukäteen on syytä selvittää myös tarkastuksen tekijä (oma henkilökunta/tarkastuslaitos) ja häneltä mahdollisesti vaadittava pätevyys. Mikäli turva-automaatiota muutetaan, käydään läpi uudelleen kaikki ne elinkaaren vaiheet, joihin muutos vaikuttaa. Uusimiseen rinnastettavista, kemikaaleihin liittyvistä muutoksista tulee tehdä ilmoitus valvontaviranomaiselle (Tukes tai pelastuslaitos). Painelaitteiden varolaitteita muutettaessa on oltava yhteydessä tarkastuslaitokseen ja hyväksytettävä muutos muutostarkastuksella. Arvioidaan, vastaako käyttö ja ylläpito määritysvaiheessa asetettuja vaatimuksia ja todetaan järjestelmän käyttöön, ylläpitoon ja muutoksiin liittyen varautumisen riittävyys.

2.4 Dokumentointi

Turvallisuuteen liittyvällä dokumentoinnilla varmistetaan riittävät tiedot kaikissa elinkaaren vaiheissa, jotta järjestelmä on toteutettavissa ja hallittavissa. Dokumentointi on edellytys sille, että järjestelmien ja riskin vähennyksen riittävyys voidaan todentaa ja arvioida. Turvallisuuteen liittyvä dokumentaatio muodostetaan omaksi selkeäksi kokonaisuudeksi. Dokumentoitavia asioita ovat suunnitelmat, määrittelyt ja kuvaukset sekä raportit (esim. kokonaisuuden turvallisuussuunnitelma ja toiminnallisen turvallisuuden arviointi).

Tarvittavia dokumentteja:
- tulokset vaara- ja riskianalyyseistä sekä niihin liittyvät lähtötiedot tai oletukset
- turvallisuussuunnitelma (jolla osoitetaan tavoitteisiin pääseminen)
- tiedot turvatoimintojen toteuttamiseen liittyvistä laitteista ja vaatimuksista
- suunnitteluun, käyttöönottoon, testaamiseen sekä kelpuutukseen liittyvät asiat
- menettelyt ja organisaatiot, jotka liittyvät turvatoimintojen toteuttamiseen, käyttöön ja ylläpitoon
- muutosmenettelyyn liittyvät vaatimukset ja toteutukset
- määräaikaiskoestus /-testaus (suunnitelma, ohje ja raportit).

3. Eri osapuolet turva-automaatiojärjestelmän toteuttamisessa

3.1. Toiminnanharjoittaja

Vastuu turva-automaatiojärjestelmän kannalta oleellisten kemikaali- ja prosessitietojen sekä vaatimusmäärittelyn antamisesta on toiminnanharjoittajalla (omistaja/haltija/tilaaja). Toiminnanharjoittajalla tulee olla määriteltynä järjestelmälliseen hallintaan liittyen menettelyt sekä uutta turva-automaatiojärjestelmää, että vanhoihin järjestelmiin tehtäviä muutoksia ja ylläpitoa varten. Vaarojen tunnistaminen ja riskien arviointi ovat oleellinen osa menettelyjä, joiden perusteella järjestelmät suunnitellaan ja kunnossapito toteutetaan.

Toiminnanharjoittaja on ensisijaisesti vastuussa myös järjestelmän käytönaikaisesta kunnossapidosta. Kun halutaan uusia tai muuttaa olemassa olevia järjestelmiä, toiminnanharjoittaja hankkii usein määrittelyn, suunnittelun ja itse järjestelmän toteutuksen ulkopuoliselta. Tällöin toiminnanharjoittajan tehtävänä on huolehtia siitä, että toteutukselle esitetään riittävät vaatimukset. Käytössä olevien järjestelmien tai niihin tehtävien muutosten ja kunnossapidon riittävyys sekä asianmukaisuus tulee pystyä osoittamaan.

Toimittajien valinnoissa on kiinnitettävä huomiota laadun hallintaan sekä kykyyn tehdä turvallisuuteen liittyviä toteutuksia. Sopimukseen on siten syytä kirjata mm. vaatimustenmukaisuuden osoittamiseen liittyvät asiat, esimerkiksi miten ja kuka tekee eri vaiheiden arviointeja. Toimittajilta on vaadittava todettuihin riskeihin ja valittuun turvallisuuden eheystasoon nähden riittävät osoitukset järjestelmän luotettavuudesta ja turvatoimintojen vikasietoisuudesta.

Kemikaalisäädökset edellyttävät uudelle laitokselle tai toiminnassa olevien laitosten turva-automaation uusimiselle Tukesin lupa- tai ilmoitusmenettelyä. Turva-automaatiosta on selvitettävä hakemuksessa mm. sen toteutusperiaatteet (esim. käytettävät standardit tai ohjeet) sekä menettelyt (projektin hallinta, arvioinnit jne), joilla toiminnanharjoittaja varmistaa, että toteutus tullaan tekemään esitettyjen periaatteiden mukaisesti ja laitoksen toimintaan liittyvät riskit huomioon ottaen.

Toiminnanharjoittajan on oltava yhteydessä riittävän aikaisessa vaiheessa lupaviranomaiseen tai vaatimustenmukaisuuden arvioinnin tekevään tahoon ja sovittava menettelyistä

3.2. Turva-automaation toimittaja ja valmistaja

Turvatekniikan toteuttaminen edellyttää ilman säädösvaatimuksiakin laadunvarmennukseen liittyvien periaatteiden noudattamista ja siten myös toteutukseen liittyviä auditointeja sekä soveltuvuuden osoittamista (esim. arviointi). Laadunvarmistuksen periaatteilla, joita ovat ennakkosuunnitelmat, kokonaisuuden elinkaaren kattavat laadunvarmistustoimet sekä kattava dokumentointi, osoitetaan kyky täyttää vaatimukset.

Painelaitteiden osalta vastuu on valmistajalla *”Sen, joka saattaa markkinoille painelaitteen (sekä siihen liittyvän varolaitteen tai turvajärjestelmän), on voitava osoittaa, että laite tai järjestelmä sekä sen suunnittelu ja valmistus täyttävät säädetyt vaatimukset”.* Toiminnanharjoittajan tulee huolehtia oikean sekä riittävän vaatimusmäärittelyn toimittamisesta valmistajalle. Turva-automaatiojärjestelmän toimittajan on toimitettava sellainen laite tai järjestelmä, joka vastaa toiminnanharjoittajan esittämiä vaatimusmäärittelyjä ja täyttää säädösten vaatimukset.

Prosessilaitosten tai tuotantolinjojen laitekokonaisuudet kootaan usein yksittäisistä laitteista, mukaan lukien turva- ja varolaitteet. Mikäli painelaitteiden laitekokonaisuuteen kuuluu turva-automaatiojärjestelmä, luokitellaan myös se painelaitteeksi. Yksittäiset painelaitteiden valmistajat vastaavat toimittamistaan laitteista. Turva-automaatiolaitteiden ja järjestelmän asentamisesta (ja valmistamisesta) laitokseen vastaa järjestelmän toimittaja tai laitekokonaisuuden valmistaja. Laitekokonaisuuden valmistaja vastaa kokonaisuuden vaatimustenmukaisuudesta, ja valmistajan on varmistettava liitettävien painelaitteiden asianmukaisuus ja soveltuvuus laitekokonaisuuteen.

Turva-automaatiotoimittajan tulee toteutuksen eri vaiheissa noudattaa edellisissä luvuissa esitettyjä vaatimuksia sekä alan hyviä käytäntöjä.

Painelaitteet, joissa on noudatettava direktiivin olennaisia turvallisuusvaatimuksia, luokitellaan riskin mukaan neljään luokkaan. Varolaitteet kuuluvat näistä vaativimpaan luokkaan. Luokan perusteella määräytyy laitteen arviointiin käytettävä arviointimenettely, johon perustuen vaatimustenmukaisuus osoitetaan.

Painelaitteista muodostuvan laitekokonaisuuden vaatimustenmukaisuus on osoitettava ja siinä on oltava CE-merkintä. Myös turva-automaatiojärjestelmässä on tarvittaessa oltava CE-merkintä. Mikäli turva-automaatiojärjestelmä on osa laitekokonaisuutta, niin CE-merkintää ei erikseen edellytetä (mutta se voi olla laitteessa). CE-merkinnällä laitteen tai laitekokonaisuuden valmistaja osoittaa, että kaikki lakisääteiset velvollisuudet (kaikki direktiivit) on täytetty – koskien myös turva-automaatiota.

CE-merkintää ei kuitenkaan sovelleta, jos painelaitteiden asennuksesta vastaa käyttäjä. Näitä ovat tyypillisesti korjaus- ja muutostyöt. Tällöin tarkastuksiin käytetään kansallista lainsäädäntöä eli KTMp 953/1999, 37§ Painelaitteen asennus-, korjaus- ja muutostyöt.

3.3. Viranomainen

Tukes (Turvatekniikan keskus) toimii Suomessa toimialansa teknisen turvallisuuden ja luotettavuuden valvontaviranomaisena. Toimialoihin kuuluvat mm. vaarallisten kemikaalien teollinen käsittely ja varastointi sekä painelaitteet ja paineelliset järjestelmät. Tehtävänä on markkinoilla olevien tuotteiden, laitteistojen, laitosten ja teknisten palveluiden valvonta.

Tukes myöntää luvat laajamittaista vaarallisten kemikaalien teollista käsittelyä ja varastointia harjoittaville laitoksille. Myös sellaisille muutoksille ja laajennuksille, jotka voidaan rinnastaa uuden laitoksen rakentamiseen, on haettava Tukesilta lupa.

Toiminnanharjoittaja esittää lupahakemuksen tai muutosilmoituksen yhteydessä suunnitelmat turva-automaatiojärjestelmän toteutuksen periaatteista ja riittävyydestä suunniteltuun tarkoitukseen sekä järjestelmän käytön aikaisista tarkastusmenettelyistä. Tukes tarkastaa tuotantolaitoksen ennen käyttöönottoa ja tekee laitoksiin määräaikaistarkastuksia. Tarkastuksissa

selvitetään, onko turva-automaation toteutus ja kunnossapito säädösten vaatimusten mukaista.

Tukes vastaa painelaitteiden markkinavalvonnasta Suomessa ja valvoo niiden käytön turvallisuutta sekä hyväksyy ja valvoo toimialansa kansallisia tarkastuslaitoksia.

3.4 Tarkastuslaitos

Tarkastuslaitosten tehtävänä on varmistaa laitteiden ja laitteistojen tekninen turvallisuus ja luotettavuus silloin, kun laitteita ja laitteistoja valmistetaan ja otetaan käyttöön sekä sen jälkeen niitä käytettäessä. Painelaitteiden turva-automaatiojärjestelmän arvioiminen, erityisesti laitekokonaisuuksien arvioinnissa ja määräaikaistarkastuksissa, kuuluu tarkastuslaitoksen tehtäviin. Arviointia tehdään myös kohteissa, jotka eivät ole pelkästään painelaitelainsäädännön kohteita (esim. kemian laitokset ja prosessiteollisuus). Näissä kohteissa on varmistettava, että arvioijan osaaminen sovellusalueelle on riittävää. Arvioinnista sovittaessa on määritettävä selkeästi, millaiset vaatimukset ja osaamisalueet arviointiin kohdistuvat, ja niiden on oltava kaikkien osapuolten tiedossa.

Painelaitteita tarkastavat tarkastuslaitokset, joita ovat ilmoitetut laitokset ja hyväksytyt laitokset.

Ilmoitettu laitos arvioi markkinoille saatettavien painelaitteiden tai laitekokonaisuuksien vaatimustenmukaisuutta ja tekee mahdollisia erityistehtäviä. Vaatimustenmukaisuuden arviointiin sisältyy painelaitetyyppien, suunnitelmien, valmistettujen painelaitteiden ja laatujärjestelmien hyväksymisiä sekä laatujärjestelmien ja valmistajan tekemien loppuarviointien valvontaa.

Hyväksytty laitos tekee painelaitteiden käyttöön liittyviä tarkastuksia ja mm. seuraavia säädettyjä toimenpiteitä: painelaitteiden määräaikaistarkastukset, kattilalaitosten vaaran arvioinnin asianmukaisuuden tarkastus, kattilalaitosten käytön valvojien pätevyyskirjan antaminen, käytössä olevien painelaitteiden asennus-, korjaus- ja muutostöiden tarkastukset.

Tukesin Internet-sivuilla (www.tukes.fi) on luettelo ilmoitetuista laitoksista ja hyväksytyistä laitoksista.

Tarkastuslaitokset tekevät myös varastosäiliöiden rakennetarkastuksia, maakaasuputkistojen tarkastuksia sekä nestekaasusäiliöiden käyttöönottotarkastuksia. Tarkastuslaitos voi toimia myös kemikaalikohteissa arvioijana.

3.5. Arvioija

Prosessilaitoksen turva-automaatiojärjestelmän arvioijana voi toimia pätevyyksiensä mukaisesti tarkastuslaitos (ilmoitettu laitos, hyväksytty laitos) tai muu valmistuksesta riippumaton ja pätevä osapuoli. Vaatimustenmukaisuuden osoittamiseen liittyvät asiat tulee selvittää hyvissä ajoin, esim. miten ja kuka eri vaiheiden arviointeja tekee. Tilaaja tai toiminnanharjoittaja valitsee sovellusalueelle sopivan arvioijan, mutta on suositeltavaa, että valintaa tehtäessä ollaan yhteydessä vaatimustenmukaisuuden arvioinnista vastuussa olevaan tahoon. Siten voidaan välttää resurssitarpeiden päällekkäisyys ja varmennetaan menettelyn asianmukaisuus.

Vaativien laitteiden (laitekokonaisuuksien) arviointimenettelyissä, joissa ilmoitettu laitos on mukana, turvajärjestelmien riittävyyden arvioi kyseinen ilmoitettu laitos, joka tällöin myös vastaa arvioinnista. Tarkastuslaitos voi teettää osan arvioinneistaan alihankkijoilla, jotka se on katsonut päteviksi ja joiden toimintaa se myös valvoo. Alihankinta perustuu kirjalliseen sopimukseen. Todistukset ja pöytäkirjat annetaan tarkastuslaitoksen nimissä ja vastuulla.

Arvioijan pätevyys ja osaaminen tehtävään on pystyttävä osoittamaan.

Arvioijalta edellytetään:

- hyvä tekninen ja ammatillinen koulutus, jota tarvitaan käytettävän teknologian arvioimiseen.
- riittävät tiedot tehtävää koskevista vaatimuksista (esim. säädökset ja standardit) ja riittävä kokemus tällaisten arviointien suorittamiseen
- vaadittu pätevyys laatia todistuksia ja raportteja, joilla todennetaan arviointien tulokset.

Arvioija selvittää ja todentaa sovelluksen toiminnallisen turvallisuuden ja vaatimustenmukaisuuden. Arvioija tarkastelee jokaisessa elinkaaren vaiheessa (määrittely, suunnittelu, toteutus, käyttö) suoritettuja toimia ja kyseisistä vaiheista saatuja tietoja. Arvioija arvioi, onko sovellettujen standardien tavoitteet ja säädösten vaatimukset sekä menettelyt täytetty.

4. Arviointi ja toiminnallisen turvallisuuden todentaminen

Turvalaitteille ja -järjestelmille on tehtävä asianmukainen loppuarviointi ja laadittava tarpeelliset asiakirjat (esim. vaatimustenmukaisuusvakuutus). Myös laitekokonaisuuteen kuuluvan, sähköisen, elektronisen tai ohjelmoitavan, suojaus- ja lukitustoimintoja sisältävän järjestelmän ja sen laitoskohtaisen toteutuksen asianmukaisuus on arvioitava.

Pelkkä toimintojen testaaminen tai toiminnallinen testaaminen ei ole riittävää turvallisuuden varmistamisessa, sillä järjestelmän virheet voivat olla piileviä ja virheiden esiintyminen satunnaista. Arvioitaessa järjestelmien luotettavuutta, riittävyyttä sekä soveltuvuutta kohteeseensa, on oltava varmuus myös kokonaisuuden toimivuudesta.

Arviointi on tehtävä yleensä sekä laitteille että sovellukselle. Laitearvioinnissa voidaan tyytyä etukäteen tehtyihin luotettavuuden ja turvallisuuden osoituksiin, kuten laitesertifiointeihin, joilla on osoitettu kyseisen tuotteen soveltuvuus tietynlaisiin turvatoimintoihin. Arvioinnin laajuutta määritettäessä voidaan myös huomioida kohteen oma laatujärjestelmien mukainen työ. Sovellusarvioinnin tulee kattaa kaikki toteuttamiseen liittyvät elinkaaren vaiheet, alkaen määritysvaiheesta. Sovellusarvioinnin tulee osoittaa järjestelmien luotettavuus ja soveltuvuus kyseisiin käyttöolosuhteisiin sekä antaa kaikille osapuolille varmuus turvallisuuden saavuttamisesta kyseisessä sovelluskohteessa.

Toiminnallisen turvallisuuden arvioinnissa selvitetään todistusaineiston perusteella sitä, että turvallisuuteen liittyvät järjestelmät ovat vaatimusten mukaisia, turvallisia ja riskin vähennys on riittävää. Arviointiin kuuluu turvallisuuden hallinnan ja suunnitelmallisuuden arviointi, toteuttajien pätevyyden arviointi, laitteiden soveltuvuuden arviointi sekä sovelluksen luotettavuuden ja turvallisuuden arviointi. Arviointi sisältää laitteiden sekä osaprosessien todentamista sekä kokonaisuuden kelpoistamista. Arvioija tekee lopuksi arviointilausunnon, jossa otetaan kantaa turva-automaatiojärjestelmän toiminnalliseen turvallisuuteen ja vaatimusten mukaisuuteen.

5. Pätevyysvaatimuksia

Kaikilla henkilöillä, jotka ovat tekemisissä turva-automaatiojärjestelmien kanssa, on oltava asianmukainen pätevyys, joka liittyy heidän tehtäviinsä. Koulutus-, työkokemus- ja pätevyystiedot on dokumentoitava sekä arvioitava aina suhteessa kyseessä olevaan sovellukseen ja järjestelmien vaatimuksiin sekä mahdollisiin seurauksiin järjestelmien toimimattomuudesta.

Kun arvioidaan henkilöiden pätevyyttä tehtäviensä suorittamiseen, on kiinnitettävä huomiota seuraaviin asioihin:

- tietämys lainsäädännön ja turvamääräysten vaatimuksista
- sovellusalueelle sekä teknologiaan sopiva tekninen ja turvallisuustekniikan tietämys (esim. sähkö-, elektroniikka-, ohjelmoitava elektroniikka-, ohjelmistotekniikka)
- suunnittelumenetelmien, rakenteen tai sovelluksen uutuus; mitä uudempia tai kokeilemattomampia ne ovat, sitä tiukempaa pitäisi olla pätevyyden määrityksen ja arvioinnin
- aiempi kokemus ja sen merkityksellisyys suoritettaviin nimenomaisiin tehtäviin ja käytettävään teknologiaan nähden (mitä korkeampi on vaadittu taso, sitä lähempänä pitäisi olla aikaisemmat kokemukset kyseisistä tehtävistä).

Arvioinnissa on otettava huomioon kokemus ja koulutus kyseiseen tehtävään ja sen vaatimuksiin liittyen. Koska Suomessa ei ole olemassa pätevyyden osoittavaa järjestelmää, on tekijöiltä pyydettävä tiedot aikaisemmista kokemuksista ja referensseistä kyseiseen tehtävään. Tarkastuslaitos tai ilmoitettu laitos voi esimerkiksi tapauskohtaisesti hyväksyä jonkun muun tahon tekemää arvioinnin vaatimustenmukaisuuden osoittamisessa. Ilmoitettuihin laitoksiin ja hyväksyttyihin laitoksiin sovelletaan vähimmäisvaatimuksia, jotka tulevat Tarkastuslaitosasetuksesta (890/1999).

Turva-automaatioon liittyviä keskeisiä käsitteitä

Käyttö- ja perusautomaatiojärjestelmä (engl. BPCS, basic process control system) tarkoittaa automaatiojärjestelmää, joka pyrkii pitämään prosessin normaalilla toiminta-alueella. Perusautomaatio ei sisällä turvallisuuteen liittyviä järjestelmiä ja sille asetettu turvallisuuden eheystaso (TET) vaatimus on alle yhden.

Turva-automaatiojärjestelmä (**TAJ**, engl. SIS, Safety Instrumented System) tarkoittaa turvallisuuteen liittyvää automaatiojärjestelmää, joka koostuu mittausantureista, logiikkaosasta (S/E/OE), ohjattavista kohteista (releet, venttiilit, moottorit jne.) sekä näiden välisestä kaapeloinnista. Turva-automaatiojärjestelmä on standardissa IEC 61511 käytetty termi turvallisuuteen liittyvästä järjestelmästä. Turvallisuuteen liittyvän järjestelmän turvallisuuden eheydelle asetetaan standardin IEC 61508 tai IEC 61511 mukaisesti suuremmat vaatimukset kuin perusautomaatiojärjestelmän turvallisuuden eheydelle.

Turvallisuuteen liittyvä järjestelmä (**TLJ**, engl. SRS, safety related system) tarkoittaa järjestelmää, joka toteuttaa ohjattavan laitteiston tai prosessin turvallisen tilan saavuttamiseksi tai ylläpitämiseksi tarpeelliset vaaditut turvatoiminnot. TLJ on tarkoitettu saavuttamaan yksin tai muiden S/E/OE TLJ:ien, muun teknologian TLJ:ien tai ulkoisten riskin vähennyskeinojen kanssa vaadittu turvatoimintojen tarpeellinen turvallisuuden eheys.

Sähköinen/elektroninen/ohjelmoitava elektroninen (**S/E/OE**) järjestelmä tarkoittaa kyseisellä tekniikalla toteutettua osaa TLJ:stä. Esimerkkinä tästä on tyyppihyväksytty turvallisuuskriittiseen käyttöön soveltuva ohjelmoitava logiikka.

Turvatoiminto (engl. Safety function) tarkoittaa toimintoa, joka toteutetaan S/E/OE turvallisuuteen liittyvällä järjestelmällä, muun teknologian turvallisuuteen liittyvällä järjestelmällä tai ulkoisilla riskin vähennyskeinoilla, jonka toiminnan tarkoitus on saavuttaa tai pitää ohjattavassa laitteistossa (tai prosessissa) turvallinen tila tiettyyn vaaralliseen tapahtumaan nähden.

Turvallisuuden eheyden taso (**TET**, engl. Safety Integrity level, SIL) on diskreetti taso (yksi neljästä mahdollisesta) S/E/OE turvallisuuteen liittyville järjestelmille osoitettavien turvatoimintojen turvallisuuden eheyden vaatimusten määrittämiseksi. Turvallisuuden eheystasoille käytetään asteikkoa 1:stä 4:ään, joista 4 on korkein turvallisuuden eheys.

Tehdastesti (**FAT**, engl. Factory acceptance testing) tarkoittaa yleensä järjestelmätoimittajan tiloissa suoritettavaa testausta, jossa todetaan järjestelmän vaatimustenmukaisuus ennen toimitusta asennuspaikalle.

Hyväksymistestaus (**SAT**, engl. Site acceptance testing) on turvallisuuteen liittyvän järjestelmän käyttöönoton yhteydessä tapahtuva hyväksyntätesti. Testi suoritetaan tyypillisesti lopullisella asennuspaikalla kenttälaitteet ja ohjausjärjestelmät asennettuna ja se päättyy usein järjestelmän kokonaiskelpoistukseen sekä luovutukseen loppuasiakkaalle.

Toiminnallisen turvallisuuden todennuksessa vahvistetaan tarkastamalla ja objektiivista todistusaineistoa hankkimalla, että laitteisiin, järjestelmiin ja eri työvaiheisiin kohdistuvat vaatimukset on täytetty.
Todennustoimiin kuuluvat mm.
- lähtötieto- ja suunnittelukatselmukset (kaikkien elinkaaren vaiheiden dokumentit) varmistamaan tavoitteiden ja vaatimusten noudattaminen ottaen huomioon ko. vaiheen nimenomaiset tiedot;
- suunniteltujen tuotteiden testaukset sen varmistamiseksi, että ne toimivat määritystensä mukaisesti;
- integrointitestit, joilla varmistetaan, että kaikki osat toimivat yhdessä, määritettyyn tapaan.

Kelpoistus tarkoittaa vahvistamista tarkastamalla ja ulkokohtaista (objektiivista) todistusaineistoa hankkimalla, että nimenomaiset vaatimukset tiettyyn aiottuun käyttöön tai toimintoon on täytetty. Kokonaisuuden kelpoistuksessa osoitetaan, että tarkasteltava laite tai järjestelmä täyttää kaikissa suhteissa vaatimusmäärittelyssä asetetut tavoitteet (TET, säädökset jne) ennen tai jälkeen asennuksen.

Suojaus (engl. protection) tarkoittaa pakko-ohjausta, jolla saatetaan ohjattava kohde turvalliseen tilaan olosuhteiden niin vaatiessa. Suojaus toimii riippumatta mahdollisesta lukituksesta tai uusista ohjauksista. TLJ:n toiminnot ovat tyypillisesti suojauksia.

Lukitus (engl. interlock) tarkoittaa vaaraa aiheuttavan toimenpiteen estoa, esimerkiksi estetään venttiilin avaaminen tai pumpun pysäyttäminen sekä käynnistäminen vaaratilanteessa.

TURVATEKNIIKAN KESKUS

PL 123 (Lönnrotinkatu 37)
00181 HELSINKI
puhelin 010 6052 000, faksi 010 6052 466
www.tukes.fi

Taitto: MacAD Oy / Kuvat: Lauri Mannermaa / Paino: Libris Oy, Helsinki 1/2008.