IEC 61508 osa 4, ed. 2

Määritelmät ja lyhenteet

Tärkeimpiä ja uusia määritelmiä

11.10.2010, Jouko Järvi

Automation Partners Oy

Suomennosongelmia on mm. englannin suuri sanavarasto. Esim. laitteistolle löytyy tässä kosolti sanoja, ainakin: system, subsystem, entity, unit, part, element, component, item.

3.1.9
OL:n riski

OL:sta (ohjattavasta laitteistosta) tai sen vuorovaikutuksesta OL:n ohjausjärjestelmään lähtevä riski

3 Huomautusta

3.1.12
toiminnallinen turvallisuus
se kokonaisturvallisuuden osa, joka liittyy OL:oon ja OL:n ohjausjärjestelmään ja riippuu S/E/OE turvallisuuteen liittyvien järjestelmien ja muiden riskin vähennysmenetelmien oikeasta toiminnasta

3.2.13
sähköinen/elektroninen/ohjelmoitava elektroninen, S/E/OE
perustuu sähköiseen (S) ja/tai elektroniseen (E) ja/tai ohjelmoitavaan elektroniseen (OE) teknologiaan

HUOM. Termi on tarkoitettu kattamaan mitkä tahansa ja kaikki sähköisillä periaatteilla toimivat laitteet tai järjestelmät.

ESIM.

3.4.1
turvallisuuteen liittyvä järjestelmä
nimetty järjestelmä joka sekä

– toteuttaa OL:n turvallisen tilan saavuttamiseksi tai ylläpitämiseksi tarpeelliset vaaditut turvatoiminnat; että
- on tarkoitettu saavuttamaan yksin tai muiden S/E/OE turvallisuuteen liittyvien järjestelmien ja muiden riskin vähennysmenetelmien kanssa vaadittujen turvatoimintojen tarpeellinen turvallisuuden eheys.

7 Huomautusta

HUOM. 4 Turvallisuuteen liittyvä järjestelmä voi

a) olla suunniteltu estämään vaarallinen tapahtuma (ts. jos turvallisuuteen liittyvät järjestelmät suorittavat turvatoimintansa, ei synny vahingollista tapahtumaa);

b) olla suunniteltu lieventämään vahingollisen tapahtuman vaikutuksia vähentäen näin riskiä pienentämällä seurauksia;

c) olla suunniteltu saavuttamaan a):n ja b):n yhdistelmä.

3.4.5
elementti
alajärjestelmän osa, joka käsittää yksittäisen komponentin tai minkä vain komponenttien ryhmän joka suorittaa yhden tai useamman elementti turvatoiminnan

HUOM. 1 Elementti voi sisältää laitteistoa ja/tai ohjelmistoa.

HUOM. 2 Tyypillinen elementti on tuntoelin, ohjelmoitava säädin tai toimilaite.

3.5.1
turvatoiminta
toiminta, joka toteutetaan S/E/OE turvallisuuteen liittyvällä järjestelmällä tai muilla riskin vähennysmenetelmillä, jonka toiminnan tarkoitus on saavuttaa tai pitää OL:lle turvallinen tila tiettyyn vaaralliseen tapahtumaan nähden (ks. 3.4.1 ja 3.4.2)

3.5.4
turvallisuuden eheys
todennäköisyys sille, että S/E/OE turvallisuuteen liittyvä järjestelmä suorittaa tyydyttävästi määritetyt turvatoiminnat kaikissa annetuissa olosuhteissa ja annettuna ajan jaksona

HUOM. 1 Mitä korkeampi on turvallisuuden eheyden taso sitä pienempi on todennäköisyys, että turvallisuuteen liittyvä järjestelmä epäonnistuu määritettyjen turvatoimintojen toteuttamisessa tai epäonnistuu ottamaan määritetyn tilan vaadittaessa.

HUOM. 4 Turvallisuuden eheys käsittää laitteiden turvallisuuden eheyden (ks. 3.5.7) ja systemaattisen turvallisuuden eheyden (ks. 3.5.6).

3.5.8

turvallisuuden eheyden taso,TET (SIL)

diskreetti taso (yksi neljästä mahdollisesta) vastaten turvallisuuden eheyden arvojen aluetta, missä turvallisuuden eheyden tasolla 4 on korkein turvallisuuden eheys ja turvallisuuden eheyden tasolla 1 matalin.

HUOM. 1 Neljän turvallisuuden eheyden tason tavoitteelliset vikaantumismitat (ks. 3.5.17) on määritetty IEC 61508-1:n taulukoissa 2 ja 3.

HUOM. 2 Turvallisuuden eheyden tasoja käytetään määrittämään S/E/OE turvallisuuteen liittyville järjestelmille kohdennettavien turvatoimintojen turvallisuuden eheyden vaatimukset .

HUOM. 3 Turvallisuuden eheyden taso (TET) ei ole järjestelmän, alajärjestelmän, elementin tai komponentin ominaisuus. Sanonnan ”TET *n* turvallisuuteen liittyvä järjestelmä” (missä n on 1, 2, 3 tai 4) oikea tulkinta on, että järjestelmä on potentiaalisesti kykenevä tukemaan turvatoimintoja, joiden turvallisuuden eheyden taso ylettyy n:ään.

3.5.5
ohjelmiston turvallisuuden eheys

se osa turvallisuuteen liittyvän järjestelmän turvallisuuden eheyttä, joka koskee systemaattisia vikaantumisia vaarallisella tavalla, joka johtuu ohjelmistosta

3.5.6
systemaattinen turvallisuuden eheys

se osa turvallisuuteen liittyvän järjestelmän turvallisuuden eheyttä, joka koskee systemaattisia vikaantumisia vaarallisella tavalla

HUOM. Systemaattista turvallisuuden eheyttä ei voida yleensä kvantifioida (erilailla kuin laitteiden turvallisuuden eheys, joka yleensä voidaan).

3.5.7

laitteiston turvallisuuden eheys

se osa turvallisuuteen liittyvän järjestelmän turvallisuuden eheydestä, joka koskee satunnaisia laitteiden vikaantumisia vaarallisella tavalla *[Määritelmä on virheellinen, ks. 3.6.6!]*

HUOM. Termi koskee vikaantumisia vaarallisella tavalla, ts. turvallisuuteen liittyvän järjestelmän niitä vikaantumisia, jotka huonontaisivat sen turvallisuuden eheyttä. Kaksi merkityksellistä parametria tässä yhteydessä ovat vaarallisen vikaantumisen keskimääräinen taajuus ja toimimatto-muustodennäköisyys vaateen ilmetessä. Ensin mainittua luotettavuus-parametriä käytetään , kun on tarpeen pitää yllä jatkuva ohjaus, jotta säilytetään turvallisuus, jälkimmäistä luotettavuusparametriä käytetään turvallisuuteen liittyvien suojausjärjestelmien yhteydessä.

3.6.5
satunnainen laitteistovikaantuminen
vikaantuminen, joka tapahtuu aikaan nähden satunnaisesti ja joka seuraa laitteiden yhdestä tai useammasta mahdollisesta huononemismekanismista

HUOM. 2 Satunnaisten laitevikaantumisten ja systemaattisten vikaantumisten (ks. 3.6.6) tärkeä erottava piirre on, että satunnaisista laitevikaantumisista johtuvat järjestelmän vikaantumistiheydet (tai muut sopivat mitat) voidaan ennustaa kohtuullisella tarkkuudella mutta systemaattisia vikaantumisia ei, juuri luonteensa mukaisesti, voida tarkasti ennustaa. Ts. satunnaisista laitevikaantumisista aiheutuvat järjestelmän vikaantumistiheydet voidaan kvantifioida kohtuullisella tarkkuudella, mutta systemaattisista vikaantumisista aiheutuneita ei voida tarkkaan tilastollisesti kvantifioida, koska niihin johtavia tapahtumia ei voi helposti ennustaa.

3.5.9

systemaattinen kyvykkyys

luottamuksen mitta (ilmaistuna asteikolla SK 1 - SK 4), että elementin systemaattinen turvallisuuden eheys täyttää määritetyn TET:n vaatimukset määritetyn elementti turvatoiminnan suhteen, kun elementtiä sovelletaan vaatimusten mukaisten nimikkeiden järjestelmäkäsikirjassa määritettyjen ohjeiden mukaisesti [Huom. 3 turha.]

HUOM. 1 Systemaattinen kyvykkyys päätetään viitaten systemaattisten vikojen välttämisen ja hallinnan vaatimuksiin (ks. IEC 61508-2 ja IEC 61508-3).

HUOM. 2 Mikä on merkityksellinen systemaattisten vikaantumisten mekanismi riippuu elementin luonteesta. Esim. yksinomaan ohjelmistosta koostuvaa elementtiä varten vain ohjelmiston vikaantumismekanismejä tarvitsee tarkastella. Laitteistosta ja ohjelmistosta koostuvaa elementtiä varten on välttämätöntä tarkastella sekä laitteiston että ohjelmiston systemaattisia vikaantumismekanismejä.

3.6.6
systemaattinen vikaantuminen
vikaantuminen, joka liittyy deterministisellä tavalla tiettyyn syyhyn ja joka voidaan eliminoida vain suunnittelun tai valmistusprosessin, käyttömenetelmien, dokumentoinnin tai muiden merkityksellisten tekijöiden muutoksella

HUOM. 1 Korjaava ylläpito ilman muutoksia ei yleensä poista vikaantumisen syytä.

HUOM. 2 Systemaattinen vikaantuminen voidaan saada aikaan simuloimalla vikaantumisen syytä.

HUOM. 3 Esimerkit systemaattisten vikaantumisten syistä sisältävät ihmisen virheen seuraavissa toimissa:

– turvallisuusvaatimusten erittely;
– laitteiston suunnittelu, valmistus, asennus ja käyttö;
– ohjelmiston suunnittelu, käyttöönotto jne.

HUOM. 4 Tässä standardissa turvallisuuteen liittyvän järjestelmän vikaantumiset luokitellaan satunnaisiksi laitteistovikaantumisiksi (ks. 3.6.5) tai systemaattisiksi vikaantumisiksi.

3.5.11

S/E/OE järjestelmän turvallisuusvaatimusten erittely

erittely joka sisältää turvatoimintojen ja niihin liittyvien turvallisuuden eheyden tasojen vaatimukset Ks. 3.5.12 ja 3.5.13

3.5.16
toimintatapa
tapa jolla turvatoiminta toimii, mikä voi olla joko

- **harvojen vaateiden tapa:** missä turvatoiminta suoritetaan vain vaateesta OL:n siirtämiseksi määritettyyn turvalliseen tilaan, ja missä vaateiden taajuus ei ole suurempi kuin yksi vuodessa; tai

Huomautus

- **tiheiden vaateiden tapa:** missä turvatoiminta suoritetaan vain vaateesta OL:n siirtämiseksi määritettyyn turvalliseen tilaan, ja missä vaateiden taajuus on suurempi kuin yksi vuodessa; tai
- **jatkuvan toiminnan tapa:** missä turvatoiminta pitää OL:n turvallisessa tilassa osana normaaalia toimintaa

3.5.17
tavoitteellinen vikaantumismitta
saavutettavaksi tarkoitettu vaarallisen vikaantumistavan tavoitetodennäköisyys turvallisuuden eheyden vaatimuksien suhteen, joka on määritetty jommallakummalla seuraavista

– turvatoiminnan vaarallisen vikaantumisen keskimääräinen todennäköisyys vaadittaessa (harvojen vaateiden toiminta-tavalle);
– vaarallisen vikaantumisen keskimääräinen taajuus [h^{-1}] (tiheiden vaateiden toimintatavalle tai jatkuvan toiminnan tavalle)

HUOM. Tavoitteellisten vikaantumismittojen numeroarvot annetaan IEC 61508-1:n taulukoissa 2 ja 3.

3.6.7
vaarallinen vikaantuminen
turvatoiminnan toteuttamiseen osallistuvan elementin ja/tai alajärjestelmän ja/tai järjestelmän vikaantuminen joka:

~~a)~~a) estää turvatoiminnan toimimasta vaadittaessa (vaateen toimintatapa) tai aiheuttaa turvatoiminnan epäonnistumisen (jatkuvan toiminnan tapa) siten että OL saatetaan vaaralliseen tai potentiaalisesti vaaralliseen tilaan; tai
b) alentaa todennäköisyyttä että turvatoiminta toimii oikein tarvittaessa

Formatted: Bullets and Numbering

3.6.10
yhteisvikaantuminen (CCF)
vikaantuminen, joka seuraa yhdestä tai useammasta tapahtumasta ja joka aiheuttaa useampikanavaisen järjestelmän kahden tai useamman erillisen kanavan yhtäaikaisen vikaantumisen, mikä johtaa järjestelmän vikaantumiseen

3.6.15.

turvallisten vikaantumisten osuus, TVO (SFF)

turvallisuuteen liittyvän elementin ominaisuus jonka määrittelee keskimääräisiä vikaantumistiheyksiä käyttäen turvallisten plus vaarallisten paljastettujen vikaantumisten suhde turvallisiin plus vaarallisiin vikaantumisiin. Seuraava yhtälö esittää tätä suhdetta:

$$TVO = (\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg})/(\Sigma\lambda_{S\ avg} + \Sigma\lambda_{Dd\ avg} + \Sigma\lambda_{Du\ avg})$$

Kun vikaantumistiheydet perustuvat vakio vikaantumistiheyksiin, yhtälö voidaan yksinkertaistaa muotoon:

$$TVO = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

3.6.17
vaarallisen vikaantumisen todennäköisyys vaateen ilmetessä, PFD
S/E**/**OE turvallisuuteen liittyvän järjestelmän turvallisuuden epäkäytettävyys (ks. IEC 60050-191) suorittamaan määritetyn turvatoiminnan vaateen ilmetessä OL:stä tai OL:n ohjaus-järjestelmästä

3 Huomautusta

3.6.19
keskimääräinen vaarallisen vikaantumisen taajuus tunnissa, PFH
S/E/OE turvallisuuteen liittyvän järjestelmän keskimääräinen vaarallisen vikaantumisen taajuus suorittamaan määritetyn turvatoiminnan annettuna ajanjaksona

4 Huomautusta

3.6.20
prosessin turva-aika
aika vikaantumisesta, joka tapahtuu OL:ssä tai OL:n ohjaus-järjestelmässä ja jolla on mahdollisuus aiheuttaa vaarallinen tapahtuma, aikaan mihin mennessä toimenpiteen tulee olla suoritettu loppuun OL:ssä estämään vaarallista tapahtumaa sattumasta

3.8.5
määräaikaistesti
määräaikainen testi, joka suoritetaan turvallisuuteen liittyvän järjestelmän vaarallisten piilevien vikaantumisten paljastamiseksi niin, että jos on tarpeen, korjaus voi palauttaa järjestelmän "kuin uusi" -tilaan tai niin lähelle tätä tilaa kuin käytännöllistä

4. Huomautusta

3.8.6
diagnostiikan kattavuus, DC

vaarallisten vikaantumisten osa joka paljastuu automaattisilla käytön aikaisilla diagnostiikkatesteillä. Tämä vaarallisten vikaantumisten osa lasketaan käyttäen paljastuneisiin vaarallisiin vikaantumisiin liittyviä vaarallisten vikaantumisten tiheyksiä jaettuna vaarallisten vikaantumisten kokonaistiheydellä

HUOM. 1 Vaarallisten vikaantumisten diagnostiikan kattavuus lasketaan käyttäen seuraavaa yhtälöä, missä *DC* on diagnostiikan kattavuus, λ_{DD} on paljastunut vaarallinen vikaantumistiheys ja λ_{Dtotal} vaarallisten vikaantumisten kokonaistiheys:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

HUOM. 2 Tämä määritelmä on sovellettavissa edellyttäen, että yksittäisten komponenttien vikatiheydet ovat vakioita.

3.8.17
turvallisuusohjekirja vaatimustenmukaisille nimikkeille
dokumentti joka antaa kaikki elementin toiminnalliseen turvallisuuteen liittyvän informaation määritettyjen elementin turvatoimintojen suhteen, mikä vaaditaan varmistamaan että järjestelmä täyttää IEC 61508 –sarjan vaatimukset

Määritelmiä on yhteensä 105 kpl. Tässä oli 26 kpl,
eli n. 25 %.