Toiminnallinen turvallisuus

Mitä uutta standardeissa IEC 61508

Tekn.lis. Matti Sundquist, Sundcon Oy
www.sundcon .fi

matti.sundquist@sundcon.fi

Mitä uutta standardeissa IEC 61508-1 ja -4?

IEC 61508-1 (yleistä):

- Vain pieniä toimituksellisia muutoksia.

IEC 61508-4 (termit ja käsitteet)

- Termejä ja käsitteitä on täsmennetty ja useita aivan uusia käsitteitä (vrt. Jouko Järven esitys).

Mitä uutta standardissa IEC 61508-5?

IEC 61508-5 (riskin arviointi):

- huomautus siitä, että standardissa ei anneta valmiita turvallisuuden eheyden tasoja (vain menetelmiä ja esimerkkejä)
- arvioinnin perustana on suhteellisen monimutkainen järjestelmä
- uudet käsitteet (komponenteille ”Systematic capability” jne.)
- siedettävän riskin (Tolerable risk) määrittämisessä on otettava huomioon lakisääteiset vaatimukset, käyttäjäorganisaation ohjeet jne.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

- uudet kohdat A.1 ”Henkilökohtainen riski”, A.2 ”Sosiaalinen riski” ja A.3 ”Jatkuva parantaminen” ja A.4 ”Riski profiili”.
- uusi kohta 5.4 ”Yhteisvikaantumiset ja ehdolliset vikaantumiset”
- uusi kohta A.9 ”Riskiä lieventävät (mitigating) järjestelmät”
- uusi luku B ”Menetelmien valinta turvallisuuden eheyden tason valintaan”
- uusi luku E.3 ”Kalibrointi” riskigraafin yhteydessä ja uusi taulukko E.2 riskigraafin kalibrointiin
- liite F ”LOPA” kirjoitettu kokonaan uudelleen.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Lisäksi:

- kohdassa A.5 erotellaan harvojen, tiheiden ja jatkuvien vaateiden tapaukset
- lisätty kohdat A 5.2 ja A 5.3 tiheille ja jatkuvien vaateiden tapauksille
- uusi kohta 5.5 ”Turvallisuuden eheyden tasot kun käytetään useita suojauskerroksia uusi kohta 5.4 ”Yhteisvikaantumiset ja ehdolliset vikaantumiset”

Mitä uutta standardissa IEC 61508-2

Uudet termit käytössä, esimerkiksi:

- Systemaattinen kyvykkyys (systematic cpability)

  “Systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level”

  SC 1…4, jos on toistaan riippumattomat elementit SC1 + SC1 = SC2
- Vaarallinen vikaantuminen (dangerous failure)
- Turvallinen vikaantuminen (safe failure)
- Elementin turvatoiminto (Element safety function)

Mitä uutta standardissa IEC 61508-2

Arkkitehtuurin rajoitukset:

Reitti 1_H "SFF-menetelmä"

- "To determine the maximum safety integrity level that can be claimed, with respect to a specified safety function"
- Perustuu parametreihin HFT ja SFF.
- 1H menetelmässä uutena turvallisen ja vaarallisen vikaantumisen määritelmät sekä muutettu laskentamentelmä verrattuna osassa 1 esitettävään mentelmään

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Arkkitehtuurin rajoitukset:

Reitti 2_H "Hyvät komponentit"

- "The minimum hardware fault tolerance for each subsystem of an E/E/PE safety- related system implementing a safety function of a specified safety integrity level".
- 2H on uusi menetelmä.
- Se perustuu kenttäkokemuksesta saatuihin komponenttien luotettavuustietoihin, korotettuihin luotettavuustasoihin ja laitteiden vikasietoisuuteen eri SIL-tasojen mukaisesti.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

- 2H on uusi menetelmä ja se edellyttää mm. (ja kohdan 7.4.4.3.2 ehdot täytettävä):
- HFT 2 SIL-tasolle 4
- HFT 1 SIL-tasolle 3
- HFT 1 SIL-tasolle 2 määrätylle jatkuva tai tiheiden vaateiden toimintatavan turvatoiminnolle, jos kohdan 7.4.4.3.2 ehtoja ei ole täytetty
- HFT 0 SIL-tasolle 2 määrätylle harvojen vaateiden toimintattavan turvatoiminnolle
- HFT 0 määrätylle SIL-tason turvatoiminnolle.
- Jos valitaan reitti 2H, tarvitaan luotettavuustietoja, jotka täyttävät niille asetetut vaatimukset. Kaikilla B-tyypin elementeillä on oltava diagnostiikan kattavuus vähintään 60 %.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Systemaattinen turvallisuuden eheys:

- Kolme vaihtoehtoista reittiä:
  - Reitti 1S: sytemaattisten virheiden välttäminen ja niiden hallinnna vaatimukset
  - Reitti 2S: Näyttö siitä, että sekä laitteisto että ohjelmisto on käytössä hyväksi koettu (Proven in use, PIU)
  - Reitti 3: Tämä koskee vain etukäteen kehitettyjä ohjelmistoja.
- Vaatimusten erittely (requirements specification)
- Uudessa versiossa vaaditaan aikaisemman yhden vaatimuserittelyn sijaa erilliset vaatimuserittelyt laitteille ja ohjelmistolle.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Digitaalinen tietoliikenne

- Vaatimukset valkoisen ja mustan kanavan arkkitehtuurille (mukaan lukien protokolla, palvelut ja verkon komponentit) esitetään viitatuissa standardeissa.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Toiminnallisen turvallisuuden hallinta

- Koko kohta on uudelleen kirjoitettu ja täydennetty, mm.:
  - Organisaation on nimettävä henkilöt ja määritettävä heidän vastuunsa elinkaaren eri vaiheissa
  - Vaatimukset ammattitaidosta koskien koko prosessia eikä vain toiminnallisen turvallisuuden arviointia kuten aikaisemmin osassa 1.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Sovelluskohtaiset ja muut integroidut piirit (ASICS)

- Esitetään käytettävät tekniikat ja toimenpiteet virheiden estämiseksi
- Käytettävät tekniikat ja toimenpiteet asiaan kuuluvien ominaisuuksien saavuttamiseksi opastavassa liitteessä
- Erityiset arkkitehtuurivaatimukset integroiduille piireille, jossa on sirutason redundanssia (velvoittava liite A)

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Turvallisuusohjekirja (Safety manual)

- Vaatimukset järjestelmän toimittajille (ml. integraattorit)
- Kaikki tiedot yhteensopivista osista (compliant item, alajärjestelmä tai elementti) niiden integroimiseksi järjestelmään tämän standardin vaatimusten täyttämiseksi.
- Valmistajien on laadittava turvallisuusohjekirja jokaiselle yhteensopivalle osalle ja niissä olevien tietojen osoittaminen standardin IEC 61508 mukaiseksi on dokumentoitava.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

Lisäksi:

- Diagnostiikan kattavuudelle uusia huomioon otettavia tekijöitä
- Määräaikaistestauksille uusia huomioon otettavia tekijöitä
- Liitteessä A taulukko komponenteille ja toiminnoille koskien satunnaisvikaantumisen arvioinnissa huomioon otettavia tekijöitä uusittu
- Sähköisten komponenttien suurimmat diagnostiikan kattavuudet
- Turvallisuusohjekirja (safety manual) monimutkaisille järjestelmille.
- Tietoturvaa koskevat yleiset vaatimukset.