Standardi IEC 61508-3 Ohjelmisto muutokset

Matti Sundquist
Sundcon Oy

www.sundcon.fi

Standardi IEC 61508-3 (1)

Standardissa esitetään

- vaatimukset niiden tietojen ja menettelytapojen valmisteluun, jota käyttäjä tarvitsee turvallisuuteen liittyvän **sähköisen*** järjestelmän käyttöä ja ylläpitoa varten.
- vaatimukset, jotka sen organisaation on täytettävä, joka toteuttaa turvallisuuteen liittyvän ohjelmiston muutokset.

***Tässä standardissa sähköisellä järjestelmällä tarkoitetaan sähköisiä, elektronisia ja ohjelmoitavia elektronisia järjestelmiä (E/E/PES)**

Standardi IEC 61508-3 (2)

Standardi

- on tarkoitettu käytettäväksi vasta standardien IEC 61508-1 ja IEC 61508-2 läpikotaisen ymmärtämisen jälkeen
- on sovellettavissa mihin tahansa ohjelmistoon, joka muodostaa osan turvallisuuteen liittyvästä järjestelmästä mukaan lukien käyttöjärjestelmät, järjestelmäohjelmisto, tietoliikenneverkkojen ohjelmistot, ihminen-kone vuorovaikutustoiminnot jakiinteäohjelmisto sekä sovellusohjelmisto.

Standardin IEC 61508-3 rakenne (1)

Standardin IEC 61508-3 rakenne:

Johdanto

1. Soveltamisala ja yleisesitys rakenteesta (kaaviot).
2. Standardiviittaukset (standardin IEC 61508 muihin osiin).
3. Määritelmät esitetään standardissa IEC 61508-4.
4. Standardinmukaisuus: viittaus standardin IEC 61508-1 kohtaan 4.
5. Dokumentaatio: viittaus standardin IEC 61508-1 kohtaan 5.
6. Lisävaatimukset (vrt. IEC 61508-1) toiminnallisen turvallisuuden hallintaan ohjelmiston kehittämisessä

Standardin IEC 61508-3 rakenne (2)

Standardin IEC 61508-3 rakenne:

7. Ohjelmiston turvallisuuden elinkaaren vaatimukset .

   7.1 Yleisesitys kaavioilla ja sen sitä selittävällä taulukolla.

   7.2 *Ohjelmiston turvallisuusvaatimusten määrittely (Safety Requirements Specification, SRS)* .

   7.3 *Järjestelmän turvallisuuden kelpuutussuunnitelma ohjelmiston osuudelle (Validation Plan for Software Aspects of System Safety).*

   7.4 Ohjelmiston suunnittelu ja kehittäminen.

   7.5 Ohjelmoitavan elektroniikan integrointi.

Standardin IEC 61508-3 rakenne (3)

Standardin IEC 61508-3 rakenne:

- 7.6 Ohjelmiston käytön ja muutosten proseduurit.
- 7.7 Järjestelmän turvallisuuden kelpuutus ohjelmiston osuudelle.
- 7.8 Ohjelmiston muutokset.
- 7.9 Ohjelmiston todentaminen.

8. Toiminnallisen turvallisuuden arviointi.

Liitteet…

Standardin IEC 61508-3 rakenne (3)

Standardin edellisen ja tämän version liitteet:

- Annex A (normative) Guide to the selection of techniques and measures
- Annex B (informative) Detailed tables
- Annex C (informative) Properties for software systematic capability

Standardin IEC 61508-3 rakenne (3)

Standardin uudet liitteet D…G:

- Annex D (normative) Safety manual for compliant items – additional requirements for software elements
- Annex E (informative) Relationships between IEC 61508-2 and IEC 61508-3
- Annex F (informative) Techniques for achieving non-interference between software elements on a single computer
- Annex G (informative) Guidance for tailoring lifecycles associated with data driven systems.

Standardin IEC 61508-3 liite A

Useille standarditekstin kohdan 7 vaatimusten täyttämiseen liittyvistä tekniikoista ja toimenpiteistä esitetään lisätietoja normatiivisessa liitteessä A ”Ohje tekniikoiden ja toimenpiteiden valintaan”. Näiden tekniikoiden ja toimenpiteiden valintaan esitetään suosituksia eri SIL-tasoille:

- ei suositeltava (NR)
- suositeltava (R)
- erittäin suositeltava (HR).

Esimerkiksi kohta 7.4.7 ”Vaatimukset ohjelmistomoduulin testaukseen” liittyy taulukkoon A.5 ”Ohjelmiston suunnittelu ja kehittäminen, ohjelmistomoduulin testaus ja integrointi”

Taulukkojen A.x otsikossa on viittaus takaisin kyseiseen standarditekstin vaatimusten kohtaan.

Standardin IEC 61508-3 liite B

Useista standardin liitteen A taulukoissa esitettävistä tekniikoista ja toimenpiteistä esitetään edelleen yksityiskohtaisia lisätietoja informatiivisessa liitteessä B ”Yksityiskohtaiset taulukot” vastaavilla suosituksilla eri SIL-tasoille kuin taulukossa A.

Liitteen A taulukon jostakin tekniikasta ja toimenpiteestä viittaus sitä koskevaan taulukkoon B on merkitty ensimmäiseen sarakkeeseen ”Ref.” merkinnällä Taulukko B.x.

Esimerkiksi liitteen A em. taulukon A.5 toimenpide (rivi 2) ”Dynaaminen analyysi ja testaus” esitetään yksityiskohtaisemmin saman nimisessä taulukossa B.2.

Taulukoiden B otsikoissa esitetään viittaukset takaisin liitteen A taulukkojen kyseistä tekniikka ja toimenpidettä esittävään kohtaan.

Standardin IEC 61508-3 liite C

Liitteessä C ”Ohjelmiston systemaattisen suoritustason ominaisuudet” luokitellaan ohjelmiston systemaattisen suoritustason ominaisuuksia niiden aikaan saaman ”vahvuuden” (rigour) mukaisesti seuraavalla asteikolla:

- R1 vähäinen tai olematon hyväksyttävyys (SIL 1 tai 2)
- R2 hyväksyttävä/korkea luottamus (SIL 3)
- R3 objektiivinen hyväksyttävyys (SIL 4).

Liitteessä C esitetään liitteiden A ja B taulukoiden kaikkien tekniikoiden ja toimenpiteiden hyväksyttävyys/luottamus ristiintaulukoituna aiheeseen liittyvien ominaisuuksien kanssa.

Esimerkiksi liitteen C taulukon C-A.5 kohdassa (rivi 2) ”Dynamic analysis and testing” annettaan arvot R1 ominaisuuksille ”testauksen täydellisyys ja oikeellisuus”.

Systemaattinen kyvykkyys (1)

IEC 61508-4 kohta 3.5.9:

- Systemaattinen kyvykkyys (*Systematic Capability)* on luottamuksen mitta, joka ilmaisee (asteikolla SIL 1...SIL 4) täyttääkö *ohjelmiston elementin systemaattinen eheys* määritetyn SIL-tason vaatimukset elementille määritetyn turvatoiminnon suhteen, kun elementtiä sovelletaan sopivassa kohteessa elementille laaditun turvallisuuskäsikirjan ohjeiden mukaisesti.
- Standardi edellyttää, että ohjelmiston toteuttamat turvatoiminnot ja ohjelmiston systemaattinen kyvykkyys on määritetty

Systemaattinen kyvykkyys (2)

Standardi IEC 61508-3

- esittää turvallisuuden elinkaaren vaiheisiin liittyvät vaatimukset ja toimenpiteet (*ohjelmiston turvallisuuden elinkaarimalli, Safety Lifecycle Model*). Näihin vaatimuksiin kuuluu sovellettavat tekniikat ja toimenpiteet, jotka on jaettu luokkiin vaadittavan *systemaattisen kyvykkyyden* mukaisesti, laitevikojen sekä ohjelmistovirheiden välttämiseen ja hallintaan.
- *Software Aspect of System Safety = järjestelmän turvallisuuden ohjelmiston osuus*

Keskeiset dokumentit (1)

- *Software System Design Specification = ohjelmistojärjestelmän suunnitelman määrittely*
- *Software Architecture Design = Ohjelmiston arkkitehtuurin suunnitelma*
- *Software Module Test Specification = ohjelmistomoduulien testausten määrittely*

Keskeiset dokumentit (1)

- *Software System Integration Test Specification = ohjelmistojärjestelmän integraatiotestausten määrittely*
- *Software Architecture Integration Test Specification = ohjelmiston arkkitehtuurin integraatiotestausten määrittely*
- *Software/PE Integration test Specification = Ohjelmoitavan elektroniikan ohjelmiston intergraatiotestauksen määrittely (laitteisto ja ohjelmisto)*
- *Validation Plan for Software Aspects of Safety System = järjestelmän turvallisuuden kelpuutussuunnitelma ohjelmiston osuudelle*