

IEC 61508

IEC 61508

IEC

IEC 61508

IEC 61508

IEC 61508

IEC 61508

SFS 175-1

SFS 175-2

SFS 175-1

SFS 175-2

SFS 631-1

SFS 631-2

SFS 631-3

SFS 631-1

SFS 631-2

SFS 631-3

SFS 631-1

SFS 631-2

SFS 631-3

Uusi automaatiokäsikirjasarja



Automaatiokäsikirjat uudistuvat. Koko kolmiosainen standardikäsikirjasarja on saatavilla alkukevästä 2012. Toiminnallisen turvallisuuden ja automaatiojärjestelmien ohjelmistostandardit sekä teollisuusautomaatioverkkojen tietoturvastandardit ovat saatavissa kompaktina käsikirjasarjana – ja monet standardeista vielä suomennettuina.

SFS 631

Automaatiokäsikirjasarja, joka aiemmin tunnettiin SFS-käsikirjana 175, uudistuu ja saa uuden SFS-numeron 631 SESKOLle varatulta 6xx-alueelta. Käsikirjojen tarkoituksena on tuoda joukko kansainvälisen sähköalan standardisointijärjestön IEC:n (International Electrotechnical Commission) standardeja automaatioalalla toimivien asiantuntijoiden, automaatioalaa opiskelevien ja kaikkien automaatiotekniikasta kiinnostuneiden käyttöön. Uudessa käsikirjassa standardit on päivitetty uusimpiin saatavilla oleviin versioihin.

Ensimmäisen osan SFS 631-1

aiheena on teollisuusautomaation sanasto ja toiminnallinen turvallisuus. Merkittävä uudistus on toiminnallisen turvallisuuden standardisarjan IEC 61508 päivittäminen versioon 2.0. Ensimmäistä kertaa koko IEC 61508 -sarja tulee olemaan saatavilla yksissä kansissa ja valtaosin suomennettuna.

Toinen osa SFS 631-2 sisältää automaatiojärjestelmien ohjelmistoihin liittyviä standardeja. Jatkossa sarja laajenee vielä teollisuusautomaatioverkkojen tietoturvaan keskittyvällä osalla SFS 631-3.

Uuden automaatiokäsikirjasarjan ensimmäinen osa SFS 631-1 on saatavana loppuvuodesta 2011.

SFS-standardeja ja standardikäsikirjoja myy Suomen Standardisoimisliitto SFS ry, puh. 09 1499 3353, <http://sales.sfs.fi/>.

IEC ja EN-standardeja välittää SESKO, puh 09 6963970, www.sesko.fi. Lisätietoja antaa Jukka Alve, SESKO ry, puh. 09 696 3965.



SESKO

Toiminnallisen turvallisuuden perustandardien IEC 61508 laatiminen alkoi parisenkymmentä vuotta sitten ja ensimmäinen versio julkaisiin 2000-luvun alussa. Standardi saavutti suuren suosion eri turvallisuuteen liittyvien järjestelmien suunnittelijoiden, laitetoimittajien ja käyttäjien keskuudessa. Monien alojen omat toiminnallisen turvallisuuden standardit perustuvat standardiin IEC 61508, esim. prosessiteollisuus, voimalaitokset, rautatiet, lääkintälaitteet sekä koneet.

Uudistetun toiminnallisen turvallisuuden standardisarjan IEC 61508 Ed 2.0 osat 0, 1, 2, 3, 4 ja 5 käännetään suomeksi.

Useita IEC 61508:n osia koskee uudistus, jonka mukaan sähköisen/elektronisen/ohjelmoitavan elektronisen järjestelmän turvallisuuden vaatimusmäärittelyt on jaettu kahteen erilliseen dokumenttiin: järjestelmän turvallisuusvaatimusmäärittely ja järjestelmän suunnitelluvaatimusmäärittely. Uutena kohtana standardisarjassa on myös vaatimus järjestelmän elementtejä koskevasta turvallisuuskäsikirjasta, joka on edellytyksenä elementtien käytölle järjestelmässä.

Osan kaksi uudistuksiin kuuluu nyt ASIC-piirin sisällyttäminen standardin soveltamisalaan. Myös laitteiston arkkitehtuurirajoitusten käsittelyyn annetaan aikaisemmalle "reitille" vaihtoehtona uusi "reitti", joka perustuu kenttäpalautteen perusteella saatuun elementtien luotettavuusdataan.

Osaan kolme on tehty suurimmat muutokset, jotka koskevat toiminnallisen turvallisuuden vaatimuksia sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien ohjelmistolle. Standardiin on lisätty ohjelmisto-elementeille käsite "systemaattinen kyvykkyys", joka korvaa aikaisemmin siinä yhteydessä käytetyn turvallisuuden eheystason.

Ajatuksena on, että ohjelmistoelementtejä voidaan kehittää käytettäväksi erilaisissa turvallisuuteen liittyvissä järjestelmissä, vaikka koko järjestelmältä vaadittu turvallisuuden eheystaso ei välttämättä ole tiedossa ohjelmistoelementtiä kehitettäessä. Peruseriaate on, että systemaattiselta kyvykkyydeltään määrättyä tasoa olevia ohjelmistoelementtejä voidaan käyttää järjestelmässä, jolta vaadittu turvallisuuden eheyden taso on tätä tasoa tai matalampi. Joissakin tapauksissa ohjelmistoelementtiä voidaan tosin käyttää myös korkeamman vaatimustason järjestelmässä, jos ohjelmistoelementtiä käytetään yhdessä muiden elementtien kanssa.

Osassa kolme esitetään ohjelmistoelementin systemaattisen kyvykkyuden osoittamiseksi kolme reittiä:

- 1) ohjelmistoelementti on kehitetty standardin mukaisesti,
- 2) ohjelmistoelementti on käytössä turvallisesti todistettu, tai
- 3) entuudestaan olemassa oleva ohjelmistoelementti, jota ei ole kehitetty standardin mukaisesti, mutta joka täyttää standardissa kuvatut vaatimukset. Kolmas näistä reiteistä on täysin uusi.

Uutena osassa kolme on kattavat taulukot ohjelmiston turvallisuusvaatimusten määrittelyn, ohjelmistosuunnittelun ja testauksen tekniikoista ja toimenpiteistä sekä todentamisesta, kelpuutuksesta ja muutosten hallinnasta. Systemaattisen kyvykkyuden arvioimiseksi on mukana taulukot ohjelmistolta vaadittavista ominaisuuksista ja suositukset käytettävistä tekniikoista ja toimenpiteistä riittävän tason saavuttamiseksi.

Osassa neljä esitetään uusia termejä, ja osassa viisi riskin arviointia on täydennetty mm. riskin arviointimenetelmien kalibrointia esittelevällä luvulla. Myös opastavat osat 6 ja 7 on päivitetty.

Käsi­kirjat on laatinut SESKOn komitea SK 65, Teollisuusprosessien ohjaus. Komitean puheenjohtaja *Matti Sundquist* kuvaa uuden käsi­kirjasarjan ensimmäisen osan tärkeimpiä uudistuksia näin:

"Nyt koko standardisarja IEC 61508 on uusittu runsaiden käyttökokemusten ja parannusehdotusten pohjalta. Uusi toinen versio on nyt käytettävissä auttamaan kaikkia turvallisuuskriittisten järjestelmien ja komponenttien valmistajia sekä käyttäjiä toiminnallisen turvallisuuden koko elinkaaren hallinnassa, kehittämisessä ja suunnittelussa. Standardisarjassa IEC 61508 esitetään toiminnallisen turvallisuuden periaatteiden ja vaatimusten ohella menetelmiä ja toimenpiteitä sekä käytettävissä olevia työkaluja vaatimusten täyttämiseen. Standardisarja IEC 61508 soveltuu myös opiskeluaineistoksi mm. turvallisuuden hallintamenetelmistä, luotettavuustekniikoista, ohjelmistokehityksestä sekä komponenttien soveltamisesta vaativiin kohteisiin."