



IEC 61508 ED3 Committee Draft for Voting (CDV) päivityksen tilanne

Janne Peltonen, 4.6.2025, Tukes, Helsinki

kiwa

Yleistä

Toiminnallisen turvallisuuden kattostandardi IEC 61508 määrittelee toiminnallisen turvallisuuden vaatimukset turvallisuuteen liittyvien järjestelmien toteutuksille

- Kattostandardin IEC 61508 asema on IEC:n mukaisesti ”Basic Safety Publication”
- Tarkoitettu eri sovellussektorien standardien kehittämisen pohjaksi

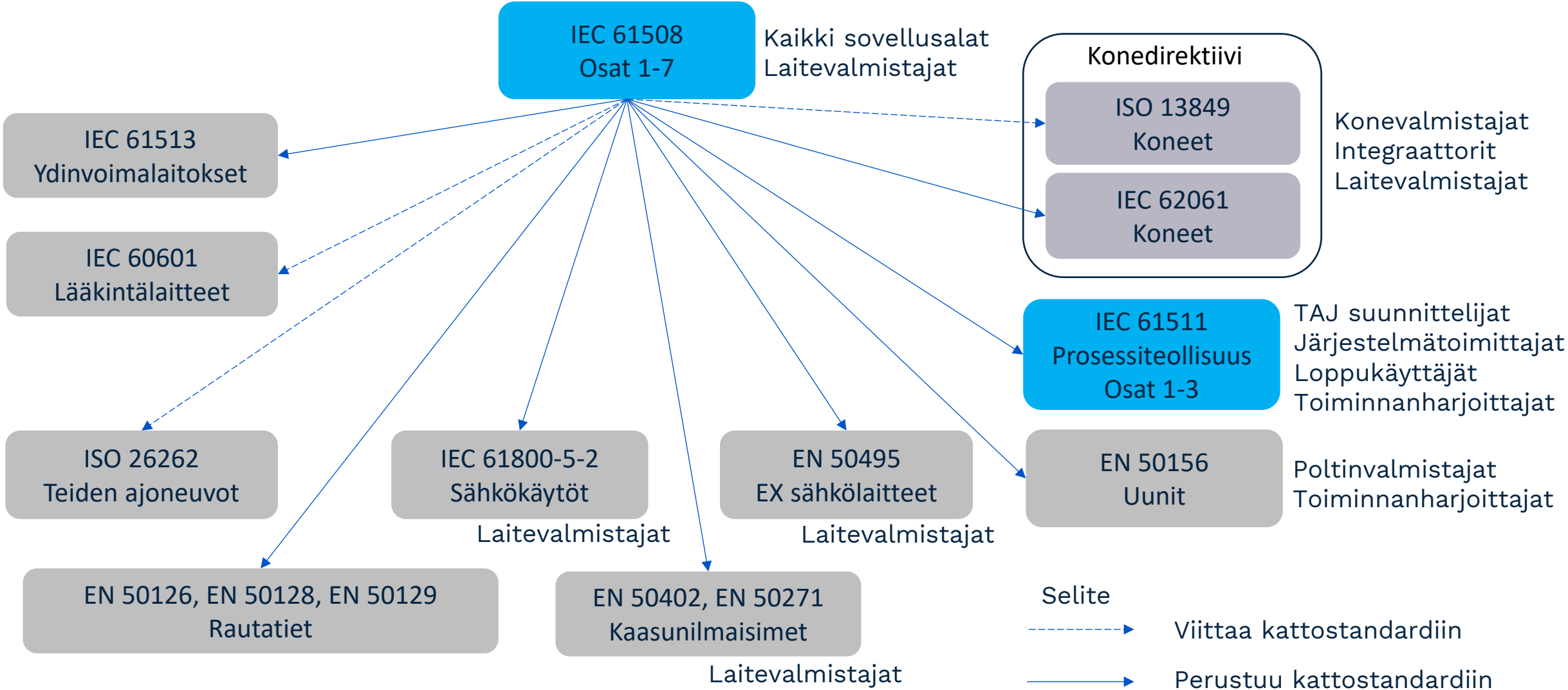
Standardin IEC 61508 keskeisiä periaatteita ovat riskilähtöinen lähestymistapa turvatoiminnoilta vaaditun suorituskyvyn määrittämiseksi ja elinkaarimalliin pohjautuva toiminnallisen turvallisuuden hallinta

Suomessa toiminnallisen turvallisuuden standardeja myy SFS (<https://sfs.fi/>)

Tämä esitys käsittelee esimerkinomaisesti kattostandardin IEC 61508 kolmannen painoksen kehitystyön mukanaan tuomia uudistuksia CDV-luonnosversion perusteella

Suomessa IEC 61508 standardisarjan kehittämiseen voi osallistua SESKO SK65 komiteajäsenenä

Kattostandardi ja sovellusstandardit



IEC 61508 standardisarja ED3

Standardien päivityksen tilanne

- IEC 61508-standardisarjan kolmannen painoksen (Edition 3) kehitystyö on edennyt äänestysvaiheeseen
 - Committee Draft for Vote (CDV)-äänestysvaihe päättyy toukokuun-kesäkuun aikana
 - Sisällöllisiä muutoksia/lisäyksiä ei tulisi enää esittää CDV-äänestysvaiheessa
- Standardien luonnokset etenevät puoltavien CDV-äänestysvaiheen tulosten jälkeen viimeiseen Final Draft International Standard (FDIS)-äänestysvaiheeseen
 - CDV-äänestystulokset voivat vaihdella eri standardin osien välillä
 - Standardisarjan eri osille on annettu kansallisilta komiteoilta sadoittain kommentteja
 - Standardisarjan eri osien ja eri työryhmien välinen koordinointi voi aiheuttaa viiveitä
 - Kokemusperäisesti arvioiden standardisarjan julkaisu tuskin tapahtuu vuonna 2025

IEC 61508 standardisarja ED3

Standardisarian osat

- IEC 61508-1 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
- IEC 61508-2 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61508-2-1 ED1
 - Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2-1: Requirements for complex semiconductors
- IEC 61508-3 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements
- IEC TR 61508-3-3 ED1
 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3-3: Object-oriented software in safety-related systems

IEC 61508 standardisarja ED3

Standardisarian osat

- IEC 61508-4 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
- IEC 61508-5 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levelsIEC 61508-2-1 ED1
- IEC 61508-6 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508)
- IEC TR 61508-7 ED3
 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures

IEC 61508 standardisarja ED3

Standardien soveltamisalat

- Osan 1 soveltamisala käytännössä ennallaan
 - Maininta kyberturvallisuuden huomioon ottamisesta elinkaaren aikana
 - Ei aseta kyberturvallisuusvaatimuksia vaan viittaa standardisarjoihin IEC 62443 sekä ISO/IEC 27000
 - Lääkinnällisten laitteiden ulosrajaus soveltamisalasta poistettu
- Osien 2, 3, 4, 5, 6 ja 7 soveltamisalat ovat ennallaan
 - Osa 6 sisältää lisää liitteitä esimerkkeinä

CD IEC 61508-1 ED3 (velvoittava)

Yleiset vaatimukset

- Lisätty maininta ”safety case” menettelystä (turvallisuusperustelusta)
- Lisätty vaatimus elinkaaren inhimillisten tekijöiden huomiointi
- Lisätty vaatimus vaatimusten hallinta (ml. viite osan 6 uusiin liitteisiin)
- Täsmennetty vaatimus henkilöiden pätevyyksien osoittaminen
- Täsmennetty vaatimus tavoitteellisen vikaantumismittan (PFD/PFH) allokointi turvatoiminnoille
- Lisätty vaatimus käyttövaiheen henkilöstön roolien määrittäminen ja inhimillisten tekijöiden varmennus

CD IEC 61508-1 ED3 (velvoittava)

Yleiset vaatimukset

- Täsmennetyt vaatimukset todennuksen ja kelpuutuksen riippumattomuus (ml. viite uuteen liitteeseen B)
- Lisätty vaatimus suunnittelu- ja arviointityökalujen toiminnallisen turvallisuuden arviointi
- Uusi kappale toiminnallisen turvallisuuden auditointi
 - Menettelytapojen noudattaminen ja soveltuvuus
 - Elinkaaren kaikkien vaiheiden auditointi
 - Auditoidijien pätevyys
- Lisätty liite B Toiminnallisen turvallisuuden varmennuksen riippumattomuus

CD IEC 61508-2 ED3 (velvoittava)

Laitteistovaatimukset

- Lisätty vaatimuksia konfiguraation hallinnalle
- Lisätty sisältövaatimuksia laitteiston suunnittelun vaatimusmäärittelylle
- Lisätty vaatimus laitteisto-ohjelmisto-rajapintamäärittelystä (ml. diagnostiikka) suunnittelussa
- Lisätty tietoliikenteen vika-analyysin vaatimuksia
- Lisätty diagnostiikkatoimintojen vaatimuksia, esim. kategoriat, eheystaso, manuaalinen/automaattinen testausväli
- Täsmennetty kelpuutuksen periaatteita, paluuta elinkaaren aiempaan vaiheeseen ja tulosten raportointia

CD IEC 61508-2 ED3 (velvoittava)

Laitteistovaatimukset

- Täsmennetty muutostenhallinnan tavoitteita
- Päivitys liite A: elektromagneettisen immunitetin suunnittelu tehtävä korkealla tehokkuudella
- Päivitetty liite B: tekniikat ja menetelmät systemaattisten vikaantumisten välttämiseen, lisätty jäljitettävyystekniikat vaatimusmäärittelyn osalta
- Poistettu liitteet E-F: Erityiset arkkitehtuurivaatimukset integroiduille piireille joissa on sisäinen varmennus sekä vaatimukset tekniikoista ja menetelmistä integroiduille piireille siirretty uuteen standardisarjan osaan IEC 61508-2-1
- Lisätty uusi liite E: yhteisvikaantumisen analyysi

CD IEC 61508-3 ED3 (velvoittava)

Ohjelmistovaatimukset

- Yleisesti huomioitu iteratiiviset / inkrementaaliset kehitysmallit ja regressiotestauksen/-kelpuutuksen tarpeet
- Ohjelmistovaatimuksissa lisätty laitteisto-ohjelmisto-rajapinnan määrittely ja ohjelmiston itsensä vikaantumisen huomiointi (ml. ohjelmiston vikaantumisen analyysitekniikat, esim. SW FMEA/FTA/HAZOP)
- Lisätty vaatimus ihminen-järjestelmä-rajapinnan suunnittelusta huomioiden inhimilliset tekijät
- Uudistettu ja lisätty merkittävästi aiemmin kehitettyjen ohjelmistojen vaatimuksia
- Lisätty vaatimuksia ohjelmistoarkkitehtuurin vikakäyttäytymiseen ja mahdollisten ohjelmiston synnyttämien uusien vaarojen edellyttämien turvatoimintojen toteutukseen
- Ohjelmiston tukityökalujen vaatimuksia uudistettu

CD IEC 61508-3 ED3 (velvoittava)

Ohjelmistovaatimukset

- Päivitetty/uudistettu merkittävästi tekniikoita ja menetelmiä liitteissä A ja B
- Päivitetty/uudistettu merkittävästi systemaattisen kyvykkyyden määreiden liitettä C
- Päivitetty/uudistettu ohjelmistojen vuorovaikutuksettomuus-liitettä F
- Lisätty sovellusdatalla konfiguroitavien järjestelmien liitettä G
- Lisätty liite H: ohjelmiston offline tukityökalut
- Lisätty liite I: mallipohjainen ohjelmistokehitys
- Päivitetty/uudistettu liite J: tieto-ohjatut järjestelmät

CD IEC 61508-4 ED3 (velvoittava)

Määritelmät

- Lisätty määritelmiä
 - Komponentti: "component" = "constituent part of an element" (ml. kuva)
 - Vaatimus: "requirement" = "provision that conveys criteria to be fulfilled"
 - Vikaantumisen: "cascading failure", "detection mechanism", "no effect failure", "failure mode", "software failure", "software fault"
 - Diagnostiikka: "diagnostic function" = "function intended to detect errors in an element or subsystem and produce a specified output information or activity when a fault is detected" (ml. kategoriat), "diagnostic function failure"
 - "reliability field feedback"
 - "proof test coverage"
 - "regression testing"

CD IEC 61508-4 ED3 (velvoittava)

Määritelmät

- Lisätty määritelmiä
 - riippumattomuustasot 1-3: tekninen, hallinnollinen tai organisaation riippumattomuus
 - "functional safety assurance" (toiminnallisen turvallisuuden varmennus)
 - tekniikoiden ja menetelmien valinta : "M", "HR", "R", "PR", "NR"
- Uusittu määritelmä
 - "software offline support tool" : poistettu T1/T2/T3 luokat
- Lisätty määritelmä
 - "software technology class" : yhteys koneoppimisen (algoritmien) / tekoälyn (AI) luokituksiin
- Poistettu määritelmä
 - "software safety integrity"

CD IEC 61508-5 ED3 (opastava)

Menetelmiä eheystason määrittämiseen

- Lisätty kuvaus yleisestä järjestelmäarkkitehtuurista jossa ohjattavan laitteiston ohjausjärjestelmät
 - Toteuttavat turvallisuuteen liittyviä turvatoimintoja (on TLJ)
 - Toteuttavat turvallisuuteen liittymättömiä ohjaustoimintoja (ei ole TLJ)

CD IEC 61508-6 ED3 (opastava)

IEC 61508-2 ja IEC 61508-3 opastusta

- Lisätty viite laskentatyökalujen osalta ohjelmistotyökalujen vaatimuksiin
- Lisätty viitteet EN 61703 ja CEN ISO / TR 12489 laskentamenetelmien osalta
- Lisätty esimerkkejä harvojen vaateiden toimintatavalle
 - Osittaisiskutestaus, korjaus/testaus käynnin aikana
- Lisätty esimerkkejä tiheiden vaateiden toimintatavalle ja jatkuvalle toimintatavalle
 - Yhdistelmä tiheiden vaateiden ja harvojen vaateiden toimintatavan turvatoiminnot
- Liite B esimerkkejä laskentatekniikoista päivitetty/uudistettu merkittävästi
 - ”Boolean approach” kappale poistettu (Reliability Block, Fault Tree, Event Tree, Cause-Consequence)
 - ennalta lasketut esimerkkitaulukot poistettu
 - ”Markovian approach” ja ”Petri nets” / ”Monte Carlo” kappaleet poistettu

CD IEC 61508-6 ED3 (opastava)

IEC 61508-2 ja IEC 61508-3 opastusta

- Lisätty kappale liitteeseen B: turvallisuuteen liittyvät järjestelmät, joilla on yhteisiä toiminnallisia elementtejä
 - Turvallisuuteen liittyvien järjestelmien keskinäisen riippumattomuuden tapaukset
- Uudistettu liite D: yhteisvikaantumisen pisteytysmenetelmä
- Lisätty liite F: diagnostiikkatoimintojen vikojen sisällyttäminen PFD/PFH laskentaan
- Lisätty liite G: vikaantumistaajuuden estimointi kenttäpalautteesta
- Lisätty liite H: opastusta jämerään turvallisuusarkkitehtuuriin

CD IEC 61508-7 ED3 (opastava) Tekniikat ja menetelmät

- Muistitesti viitteitä lisätty
- Elektromagneettinen immunitaetti: viitteitä IEC 61000-1-2 ja IEC 61326-3-2 täydennetty
- “Functional Safety Assurance Role Independence” kuvaus lisätty
- Muodollisten menetelmien käyttö on viitattu uuteen standardisarjan osaan IEC TS 61508-3-2
- Ohjelmistokehityksen kirjallisuusviitteitä lisätty
- Tekoälyn (AI) viitteet rajattu pois

CD IEC 61508-7 ED3 (opastava)

Tekniikat ja menetelmät

- Uusia ohjelmiston analyysitekniikoita yhteisvioille ja ketjuuntuville vaikutuksille
- Regressiolla kelpuutuksen kuvausta täydennetty
- “Software failure analysis” tekniikoiden kuvauksia lisätty
- Yhteisvikaantumisen analyysin kuvausta täydennetty
- Liite D uudistettu: käytössä olevien ohjelmistojen tilastollinen arviointi
- Liite E poistettu: tekniikat ja menetelmät monimutkaisille integroiduille piireille siirretty uuteen standardisarjan osaan IEC 61508-2-1
- Liite G: oliopohjainen ohjelmistokehitys tulossa uusi standardisarjan osa IEC TR 61508-3-3

Kiitos mielenkiinnosta!

Janne Peltonen
Asiantuntija, Automaatioturvallisuus
T +358 50 302 5280
E janne.peltonen@kiwa.com