Committee Draft IEC 61508 ED3
Toiminnallisen turvallisuuden standardin tulevat muutokset

7.6.2023

Suomen Automaatioseura, turvallisuusjaos (ASAF)

Kiwa Inspecta

Janne Peltonen

Trust
Quality
Progress

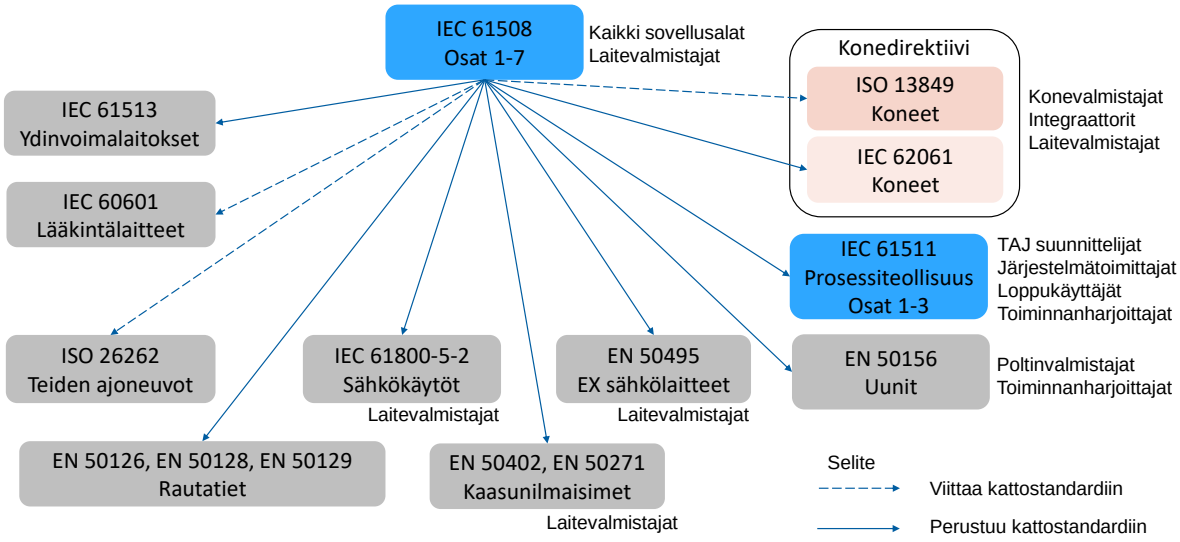
1

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 kattostandardin IEC 61508 kolmannen painoksen kehitystyön mukanaan tuomia **mahdollisia uudistuksia CD-version perusteella**
- Suomessa IEC 61508 kehittämiseen voi osallistua **SESKO SK65** komiteajäsenenä

2

Kattostandardi ja sovellusstandardit



3

Toiminnallisen turvallisuuden evoluutio

- **1960-luku: kovalangoitetut relekytkennät ja lukitusjärjestelmät**
  - Mekaaniset varolaitteet ja pneumaattiset ohjauslaitteet
  - Sähkömekaanisia järjestelmiä sovellettiin riskialtteimmissa sovellutuksissa
- **1970-luku: puolijohde-elektroniikalla toteutetut järjestelmät**
  - Prosessien vaaroja ryhdyttiin miettimään ja arvioimaan
  - Puolijohde-järjestelmiä integroitiin prosessiautomaatioon, uuden teknologian vikamuotoja ei tunnettu ja käyttökokemusta ei ollut kertynyt
  - 1976 Seveso kemikaalilaitoksen onnettomuus ja suuronnettomuuksiin varautumisen konsepti
  - 1979 Three Mile Island ydinvoimalan onnettomuus ja ”normaalien onnettomuuksien” eli monimutkaisten järjestelmien onnettomuuksien konsepti

4

Toiminnallisen turvallisuuden evoluutio

- **1980-luku: ohjelmoitavat logiikkajärjestelmät (PLC) ja hajautetut ohjausjärjestelmät (DCS)**
  - Sovellusaluekohtaiset konservatiiviset ja ennalta määräävät suunnittelusäännöt
  - Järjestelmien kyky diagnostiikkaan kasvoi
  - Saksassa standardit VDE 0801 ja DIN 19250 (AK-luokat) ja USA:ssa ISA-S84
  - Ensimmäiset turvalogiikoiden tyyppihyväksynnät Saksassa
  - 1984 TÜV julkaisu ”Microcomputer in der Sicherheitstechnik”
  - 1984 Bhopal kemikaalilaitoksen päästöonnettomuus ja yrityksen välinpitämättömyyden ja työntekijöiden sabotaasin näkökulmat ylläpidolle
  - 1986 TTK kielto ohjelmoitavien järjestelmien käytölle
  - 1986 Chernobylin ydinvoimalan onnettomuus ja turvallisuuskulttuurin konsepti
  - 1987 HSE julkaisu ”PES in safety related applications”
  - 1988 Piper Alpha porauslautan onnettomuus ja Safety Case konsepti

5

Toiminnallisen turvallisuuden evoluutio

- **1990-luku: ohjelmoitavat turvalogiikkajärjestelmät (engl. Safety Programmable Logic Controller)**
  - Turvalogiikoiden käyttö alkoi Suomessa
  - Erilaisia käyttäjien turvakonfiguraatioita PLC-toteutuksiin
  - 1994 saksalainen standardi DIN 19250
  - 1994 TTK suositus 1-1994 – IEC 61508 luonnosversion pohjalta
  - Ensimmäinen sertifiointi TTK suosituksen 1-1994 pohjalta Suomessa
  - 1996 EN 954-1 – standardi koneturvallisuuteen
  - Voimakasta kansainvälistä yhteistyötä parempien toiminnallisen turvallisuuden standardien aikaan saamiseksi
  - 1998 IEC 61508 Ed. 1.0 – kattostandardin ensimmäiset osat
  - 1999 ISO 13849-1 Ed. 1.0 – standardi koneturvallisuuteen EN 954-1 pohjalta

6

Toiminnallisen turvallisuuden evoluutio

- **2000-luku: turvalaitteiden, turvalogiikoiden ja turvaväylien sertifiointi**
  - Turvalaitteiden sertifiointi kolmansien osapuolien toimesta pääsi vauhtiin
  - Sertifioidut turvalogiikka-alustat yleistyvät markkinoilla
  - Käyttäjien ei tarvitse enää analysoida kaikkia laitteiden vikaantumisten riskejä
  - Turvalaitteiden diagnostiikka paljastaa useimmat viat omatoimisesti käytön aikana
  - IEC 61508 standardin mukaisia kenttälaitteita vähän saatavilla
  - 2000 IEC 61508 Ed. 1.0 – kattostandardin kaikki osat
  - 2003 IEC 61511 Ed. 1.0 – IEC 61508 sovellusstandardi prosessiteollisuuteen
  - 2005 IEC 62061 Ed. 1.0 – IEC 61508 sovellusstandardi koneturvallisuuteen
  - 2005 Texas City jalostamon räjähdysonnettomuus
  - 2006 ISO 13849-1 Ed. 2.0 – IEC 62061 kanssa kilpaileva standardi koneturvallisuuteen

7

Toiminnallisen turvallisuuden evoluutio

- **2010-luku: tuotesertifioinnin laajeneminen ja kyberturvallisuuden esille tulo**
  - Sertifioidut turvalaitteet, turvalogiikat, kenttälaitteet, elektroniset piirit, ohjelmistokomponentit ja ohjelmistotyökalut laajasti saatavilla markkinoilla
  - Turvalogiikoiden kapasiteetti, skaalautuvuus ja ominaisuudet kasvavat
  - 2010 IEC 61508 Ed. 2.0 – uudistettu kattostandardi
  - 2010 Stuxnet ensimmäinen teollisuuslogiikoihin kohdennettu haittaohjelma 2011
  - 2011 ISO 26262 Ed. 1.0 – IEC 61508 sovellusstandardi autoteollisuuteen
  - 2011 Fukushima Daiichi ydinvoimalan onnettomuus ja varavoiman konsepti
  - 2015 ISO 13849-1 Ed. 3.0 – IEC 62061 kanssa kilpaileva standardi koneturvallisuuteen
  - 2016 IEC 61511 Ed. 2.0 – IEC 61508 sovellusstandardi prosessiteollisuuteen
  - 2017 Triton haittaohjelma joka oli kohdennettu Triconex turvalogiikoihin
  - 2018 ISO 26262 Ed. 2.0 – IEC 61508 sovellusstandardi autoteollisuuteen

8

Toiminnallisen turvallisuuden evoluutio

- **2020-luku:**
  - **IEC 61508 Ed. 3.0 – päivitystyö on meneillään Committee Draft-vaiheessa**
  - IEC 61511 ylläpitotyöryhmä on perustettu
  - 2021 IEC 62061 Ed. 2.0 – IEC 61508 sovellusstandardi koneturvallisuuteen
  - 2023 ISO 13849-1 Ed. 4.0 – uudistettu IEC 62061 kanssa kilpaileva standardi koneturvallisuuteen
  - Uusien teknologioiden yleistyminen tai lisääntyminen
    - Ennalta kehitetyt sisäisesti varmennetut monimutkaiset piirit
    - Mallipohjainen ohjelmiston kehitys ja tarkastus
    - Sertifioidut reaaliaikaiset turvallisuuteen liittyvät käyttöjärjestelmät
    - Pilvipohjaiset turvallisuuteen liittyvät sovellusohjelmat
    - Turvallisuuteen liittyvät tekoälysovellukset

9

IEC 61508 sarja ED3
Standardien soveltamisala

- **Osan 1 soveltamisala käytännössä ennallaan**
  - Mainita kyberturvallisuuden huomioon ottamisesta elinkaaren aikana
  - Mainita ohjattavan laitteiston ohjausjärjestelmistä, jotka toteuttavat turvallisuuteen liittyviä toimintoja ja turvallisuuteen liittymättömiä toimintoja
- **Osien 2, 3, 4, 5, 6 ja 7 soveltamisala ennallaan**

10

CD IEC 61508-1 ED3 (velvoittava) Yleiset vaatimukset

- **Lisätty maininta ”safety case” menettelystä**
- **Lisätty elinkaaren inhimillisten tekijöiden huomiointi (ml. standardiviitteet)**
- **Lisätty vaatimusten hallinta (ml. viite osan 6 uusiin liitteisiin)**
- **Täsmennetty henkilöiden pätevyyksien osoittaminen**
- **Lisätty tavoitteellisen vikaantumismitan allokointi käyttövaiheeseen**
- **Lisätty käyttövaiheen henkilöstön määritys ja inhimillisten tekijöiden huomiointi**

11

CD IEC 61508-1 ED3 (velvoittava) Yleiset vaatimukset

- **Täsmennetty todennuksen ja kelpuutuksen riippumattomuutta (ml. viite osan 7 uuteen kohtaan)**
- **Lisätty suunnittelu- ja arviointityökalujen toiminnallisen turvallisuuden arviointi**
- **Uusi kappale toiminnallisen turvallisuuden auditointi**
  - Kaksi fokusaluetta
  - Elinkaaren kaikkien vaiheiden auditointi
  - Auditoijien pätevyys
- **Lisätty liite B: Toiminnallisen turvallisuuden varmennuksen riippumattomuus**

12

CD IEC 61508-2 ED3 (velvoittava) Laitteistovaatimukset

- **Lisätty vaatimuksia konfiguraation hallinnasta**
- **Lisätty sisältövaatimuksia laitteiston suunnittelun vaatimusmäärittelylle**
- **Lisätty vaatimus laitteisto-ohjelmisto rajapintamäärittelystä (ml. diagnostiikka)**
- **Lisätty vaatimus huomioida arkkitehtuurisuunnittelun synnyttämät vaaratilanteet**
- **Uudistettu tietoliikennevaatimuksia**
- **Lisätty diagnostiikkatoimintojen vaatimuksia (ml. kategoriat)**
- **Täsmennetty kelpuutuksen periaatteita ja paluuta elinkaaren aiempaan vaiheeseen**

13

CD IEC 61508-2 ED3 (velvoittava) Laitteistovaatimukset

- **Täsmennetty muutostenhallinnan tavoitteita**
- **Päivitys liite A: elektromagneettisen immuniteetin suunnittelu**
- **Päivitetty liite B: tekniikat ja menetelmät systemaattisten vikaantumisten välttämiseen**
- **Uusittu liite E: Erityiset arkkitehtuurivaatimukset integroiduille piireille joissa on sisäinen varmennus**
- **Uusittu liite F: integroidut piirit (aiemmin ASIC)**
- **Lisätty liite G: yhteisvikaantumisen analyysi**

14

CD IEC 61508-3 ED3 (velvoittava) Ohjelmistovaatimukset

- **Yleisesti huomioitu inkrementaaliset kehitysmallit ja regressiotestaus**
- **Ohjelmistovaatimuksissa lisätty ohjelmiston vikojen huomiointi**
- **Lisätty käytön aikaiset parametrien kohdalla inhimilliset tekijät**
- **Lisätty HW/SW yhteisen systeemisuunnittelun näkökohtia**
- **Lisätty aiemmin kehitettyjen ohjelmistojen vaatimuksia**
- **Lisätty viitteitä regressiotestaustarpeisiin**

15

CD IEC 61508-3 ED3 (velvoittava) Ohjelmistovaatimukset

- **Päivitetty tekniikoita ja menetelmiä-liitteitä**
- **Päivitetty systemaattisen kyvykkyyden määreiden liitettä**
- **Päivitetty ohjelmistojen riippumattomuus-liitettä**
- **Päivitetty tieto-ohjattujen järjestelmien liitettä**
- **Lisätty liite H: ohjelmiston offline tukityökalut**
- **Lisätty liite I: mallipohjainen ohjelmistokehitys**

16

CD IEC 61508-4 ED3 (velvoittava) Määritelmät

- **Lisätty määritelmiä**
  - ”component” (ml. kuva)
  - ”requirement”
  - ”cascading failure”, ”activation condition”, ”detection mechanism”, ”failure effect”, ”failure mechanism”, ”failure mode”, ”failure with plausible system behaviour”, ”software failure”, ”software fault”
  - ”diagnostic function” (ml. kategoriat), ”diagnostic function failure”
  - ”reliability field feedback”
  - ”proof test coverage”
  - ”regression testing”
  - ”safety case”

17

CD IEC 61508-4 ED3 (velvoittava) Määritelmät

- **Lisätty määritelmiä**
  - tekninen, hallinnollinen ja organisaation riippumattomuus
  - toiminnallisen turvallisuuden varmennus
  - tekniikoiden ja menetelmien valinta
- **Uusittu määritelmä**
  - ”software offline support tool”
- **Poistettu määritelmä**
  - ”software safety integrity”

18

CD IEC 61508-5 ED3 (opastava)
Menetelmiä eheystason määrittämiseen

- **Lisätty kuvaus standardin yleisestä arkkitehtuurista jossa ohjattavan laitteiston ohjausjärjestelmät**
  - Toteuttavat turvallisuuteen liittyviä ohjaustoimintoja
  - Toteuttavat turvallisuuteen liittymättömiä ohjaustoimintoja

19

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 / TR12489**
- **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
- **”Boolean approach” kappale poistettu (RBD, FTA)**
- **”States/transitions approaches” kappale poistettu (Markov, Petri)**

20

CD IEC 61508-6 ED3 (opastava)
IEC 61508-2 ja IEC 61508-3 opastusta

- **Lisätty kappale: turvallisuuteen liittyvät järjestelmät, joilla on yhteisiä elementtejä**
  - Turvallisuuteen liittyvien järjestelmien keskinäisen riippumattomuuden taso
- **Uusittu liite D: yhteisvikaantumisen pisteytysmenetelmä**
- **Lisätty liite F: diagnostiikkatoimintojen vikojen sisällyttäminen laskentaan**
- **Lisätty liite G: vikaantumistaajuuden estimointi kenttäpalautteesta**
- **Lisätty liite H: vaatimusten ja määrittelyjen erot**
- **Lisätty liite I: opastusta vaatimusten hallintaan**

21

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

- **Muistitesti viitteitä lisätty**
- **Elektromagneettinen immuniteetti: viite IEC 61000-1-2 lisätty**
- **“Functional Safety Assurance Role Independence” kuvaus lisätty**
- **Muodollisten menetelmien kuvausta täydennetty**
- **Puolimuodolliset menetelmät näennäisesti poistettu**
- **Ohjelmistokehityksen kirjallisuusviitteitä lisätty**
- **Tekoäly (AI) rajattu pois standardin soveltamisalasta**

22

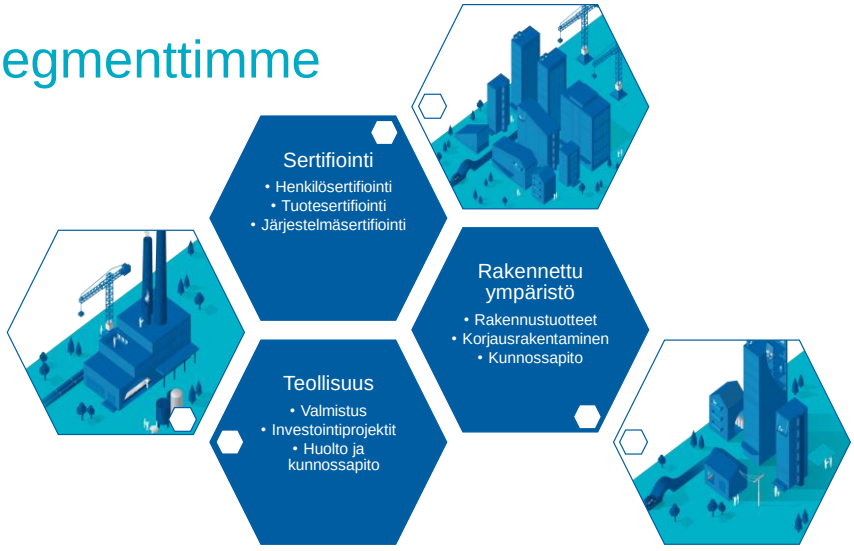
CD IEC 61508-7 ED3 (opastava) Tekniikat ja menetelmät

- **Uusia ohjelmiston analyysitekniikoita yhteisvioille ja ketjuuntuville vaikutuksille**
- **Regressiolla kelpuutuksen kuvausta täydennetty**
- **“Software failure analysis” tekniikoiden kuvauksia lisätty**
- **Yhteisvikaantumisen analyysin kuvausta täydennetty**
- **Liite D uusittu: Aiemmin kehitettyjen ohjelmistojen tilastollinen arviointi**
- **Liite E uusittu: tekniikat ja menetelmät monimutkaisille integroiduille piireille**
- **Liite H lisätty: “soft errors” opastus**

Vahvuutemme
Kokemus ja laaja palveluvalikoima

- Kiwalla on n. 70 vuoden ja Inspectalla yli 40 vuoden kokemus tarkastus-, testaus- ja sertifiointipalveluista
- Kiwa on TIC top 20 maailmanlaajuisesti, Inspecta on markkinajohtaja Pohjoismaissa
- Kiwa Inspectalla on Pohjois-Euroopan laajin palveluvalikoima

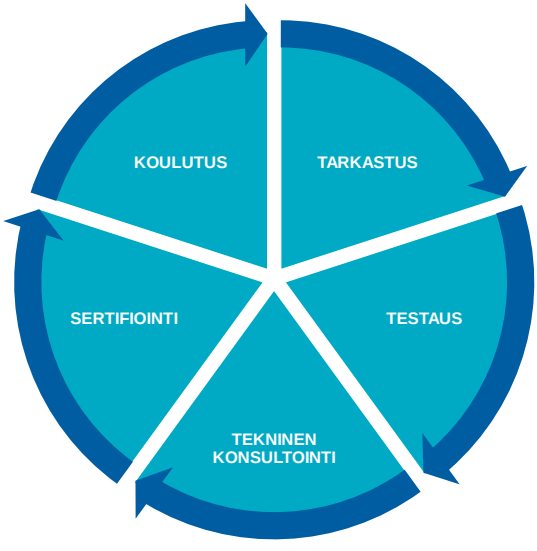
Asiakassegmenttimme



25

Palvelumme

- **Laajan palvelutarjontamme perustana ovat:**
  - Tarkastus
  - Testaus
  - Tekninen konsultointi
  - Sertifiointi
  - Koulutus
- **Toimitamme kaikkia palveluitamme myös yksittäin – parhaan hyödyn saat kuitenkin kokonaisratkaisusta, joka tekee toiminnastasi turvallisempaa, yksinkertaisempaa ja kannattavampaa.**



26

Trust, Quality & Progress