

Toiminnallisen turvallisuuden ja teollisuuden kyberturvallisuuden standardit

SESKO

25.9.2020 Jukka Alve



IEC TC 65:n ja SC 65A:n toiminnallisen turvallisuuden ja kyberturvallisuuden standardit

Toiminnallisen turvallisuuden standardit

- IEC 61508 -sarja (perusstandardi)
- IEC 61511 -sarja (prosessiteollisuus)

Kyberturvallisuuden standardit

- IEC 62443 -sarja

Toiminnallinen turvallisuus & kyberturvallisuus

- IEC TR 63069
- IEC PAS 63325

Mitä on toiminnallinen turvallisuus?

- Turvallisuus on vapautta sellaisista riskeistä, joita ei voida hyväksyä
- Toiminnallinen turvallisuus on turvallisuuden se osa, joka riippuu järjestelmän tai laitteiden oikeasta toiminnasta vasteena tiettyihin herätteisiin.
- Toiminnallinen turvallisuus perustuu aktiivisiin järjestelmiin (joista standardeissa käytetään nimityksiä turva-automaatiojärjestelmät).
- Passiivisiin järjestelmiin perustuvat turvallisuusratkaisut eivät ole toiminnallista turvallisuutta.

IEC 61508 –sarja

IEC 61508 –sarja Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus

- **IEC/TR 61508-0:fi** -- Osa 0: Toiminnallinen turvallisuus ja IEC 61508
- **SFS-EN 61508-1** -- Osa 1: Yleiset vaatimukset
- **SFS-EN 61508-2** -- Osa 2: Vaatimukset sähköisille/elektronisille/ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille
- **SFS-EN 61508-3** -- Osa 3: Ohjelmistovaatimukset
- **SFS-EN 61508-4** -- Osa 4: Määritelmät ja lyhenteet
- **SFS-EN 61508-5** -- Osa 5: Esimerkkejä menetelmistä turvallisuuden eheyden tasojen määrittämiseksi

IEC 61508 –series Functional safety of electrical/electronic/programmable electronic safety-related systems

- **IEC/TS 61508-3-1** -- Part 3-1: Software requirements - Reuse of pre-existing software elements to implement all or part of a safety function
- **SFS-EN 61508-6:en** -- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- **SFS-EN 61508-7:en** -- Part 7: Overview of techniques and measures

IEC 61511 -sarja

IEC 61511 -sarja Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille

- **IEC/TR 61511-0:2018:fi** -- Osa 0: Prosessiteollisuuden toiminnallinen turvallisuus ja IEC 61511
- **SFS-EN 61511-1:2017** -- Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset
- **SFS-EN 61511-1:2017/A1:2017** -- Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset
- **SFS-EN 61511-2:2017** -- Osa 2: Ohjeita standardin IEC 61511-1:2016 soveltamiseen
- **SFS-EN 61511-3:2017** -- Osa 3: Ohjeita vaadittavien turvallisuuden eheyden tasojen määrittämiseen
- **IEC/TR 61511-4 ed1.0 (2020-02)** Functional safety - Safety instrumented systems for the process industry sector - Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2 (suomennos tulossa)

Tulossa olevia julkaisuja toiminnallisesta turvallisuudesta

- **IEC TS 61508-3-2 ED1** Requirements and Guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation
- **IEC TS 61508-3-3 ED1** Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3-3: Requirements for object-oriented software in safety-related systems
- **IEC 63187 ED1** Functional safety - Framework for safety critical E/E/PE systems for defence industry applications

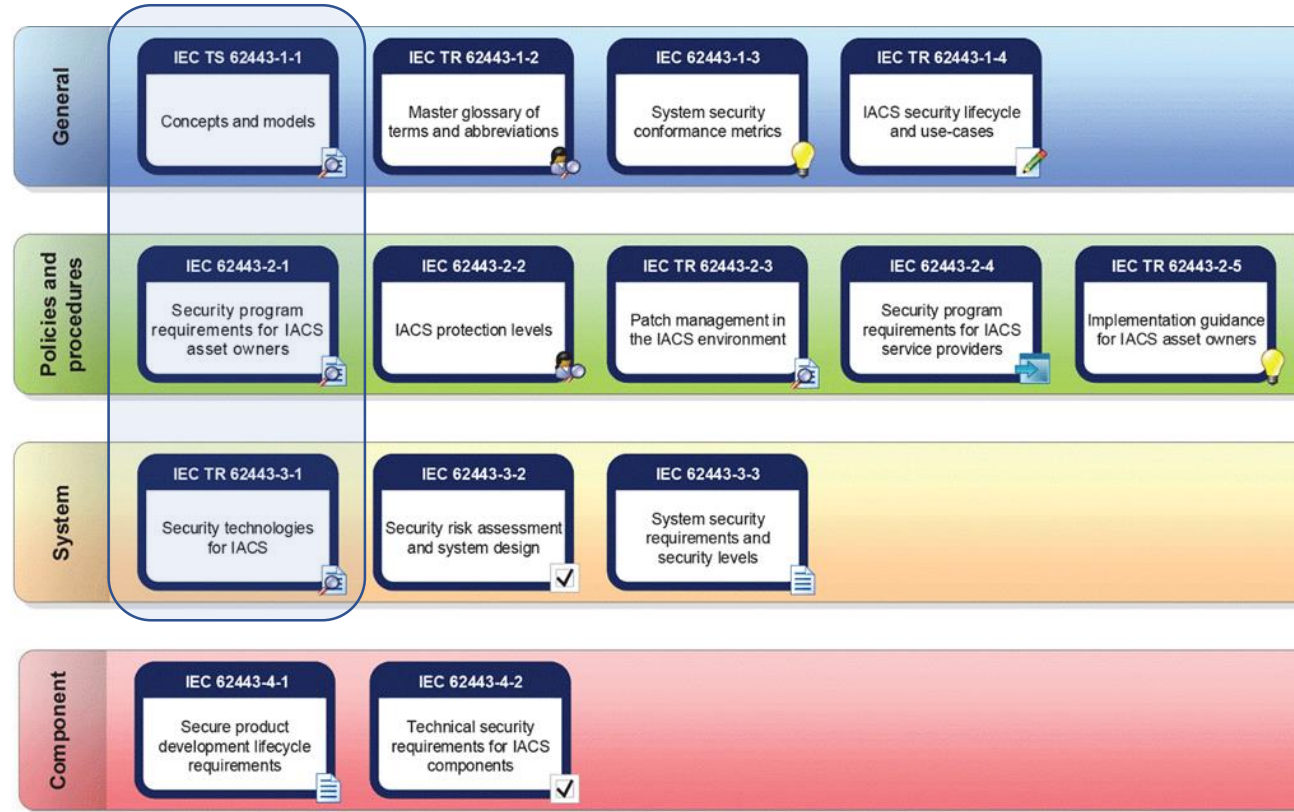
Päivityksessä huomioitavaa:

- Inhimilliset tekijät otetaan huomioon IEC 61508 -sarjan olemassa olevia osia päivitettäessä – ei erillistä osaa
- Uutena teemana tekoäly ja toiminnallinen turvallisuus – yhteistyö alkamassa komitean ISO/IEC JTC 1 SC 42 kanssa?

Mitä tarkoitetaan kyberturvallisuudella?

- Turvallisuus on vapautta sellaisista riskeistä, joita ei voida hyväksyä
- Kyberturvallisuus on sukua tietoturvallisuudelle – uhat usein verkossa
- Kyberturvallisuudesta puhuttaessa uhka kohdistuu usein terveyteen, turvallisuuteen tai ympäristöön omaisuuden lisäksi
- Jos uhka kohdistuu vain tieto-omaisuuteen, kyberturvallisuus on todennäköisesti väärä sana => ISO/IEC 27000 -sarja

IEC 62443 -sarja



IEC 62443 –sarja, suomennetut osat

- **IEC/TS 62443-1-1:fi** Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit
- **SFS-IEC 62443-2-1** Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten
- **IEC/TR 62443-3-1:fi** Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille

Ehdotettuja uusia työkohteita

- **PNW TS 65-827** Rules for IEC 62443 Profiles
- **PNW TS 65-828** Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS service providers
- **PNW TS 65-829** Security evaluation methodology for IEC 62443 – Part 4-2: Technical security requirements for IACS components

Toiminnallisen turvallisuuden ja kyberturvallisuuden yhtymäkohdat

- **CLC IEC/TR 63069:2020:fi** Teollisuusprosessien mittaus, ohjaus ja automaatio. Toiminnallisen turvallisuuden ja tietoturvallisuuden viitekehys
- **IEC PAS 63325 ED1** Lifecycle requirements for Functional Safety and Security for IACS (tulossa)

Standardeihin voi vaikuttaa

SESKOn komiteoissa

- äänestämällä uusista työkohteista (NP-vaihe)
- kommentoimalla ehdotuksia (CD- ja CDV-vaiheet)
- äänestämällä ehdotuksista (CDV, FDIS -vaiheet)

IEC:n tai CENELECin työryhmissä

- keskustelemalla työryhmissä standardiehdotusten sisällöstä asiantuntijoiden kesken
- kirjoittamalla tekstiä ehdotukseen muiden asiantuntijoiden kommentoitavaksi
- osallistumalla kansalliskomiteoiden kommenttien käsittelyyn

Lisätietoa: www.sesko.fi/osallistuminen