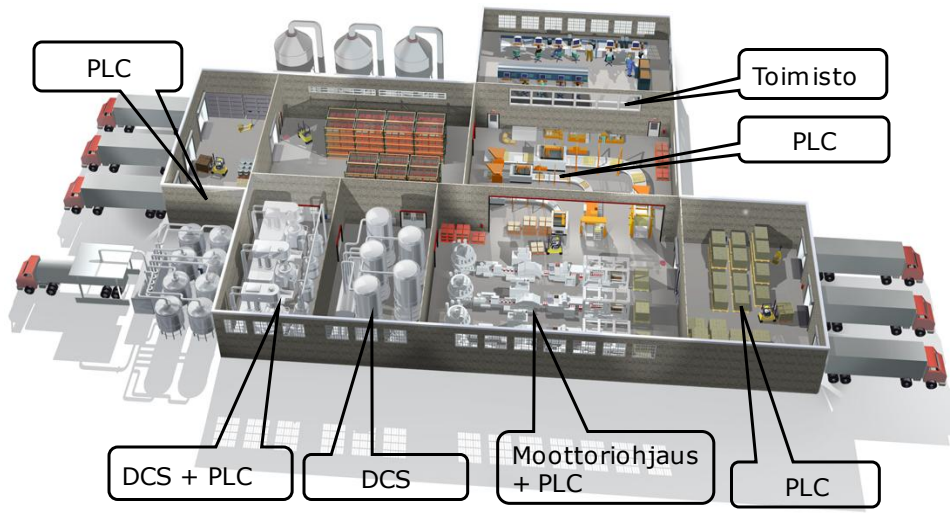
Toiminnallinen turvallisuus

Tekn.lis. Matti Sundquist, Sundcon Oy

Matti.sundquist@sundcon.fi

Tehdasautomaatio



Esimerkkejä ei-toivotuista tapahtumista

Isä puristui robotin ja liukuhihnan

SEINÄJOKI: Kevythirsi- ja paneelimökkielementtejä valmistavassa perheyrityksessä koettiin kauhunhetkiä sunnuntaina yhden jälkeen.

Etelä-Pohjanmaan poliisilaitoksen ylikonstaapeli **Pasi Vuorenmaan** mukaan toinen omistajista oli ilmeisesti näyttämässä pojalleen, kuinka työtä tehdään. Hän esitteli tuotantolinjaa ja robottia, joka siirtelee puutavaraa pisteestä toiseen. Ylättäen koneeseen tuli häiriö, ja robotti pysähtyi.

Mies meni tarkistamaan, mistä vika oli peräisin, mutta yllättäen robotti lähti käyntiin. Toimintahäiriö johti siihen, että mies jäi raskasta puutavaraa nostavan robotin ja tuotantolinjan väliin puristuksiin lapaluidensa kohdalta.

Paikalla ei ollut muita henkilöitä kuin tapahtumia todistanut poika. Vuorenmaan mukaan pojan äiti oli lähettyvillä, ja poika sai ilmoitettua hänelle tapahtumista. Äiti soitti hätäkeskukseen, ja paikalle saapuivat pelastuslai-

▸ Mariella ajelehti tunnin avomerellä sähkövian takia

Juhani Saarinen
HELSINGIN SANOMAT

▶ Viking Linen matkustajalusten viime päivien vioilla ei ole yhteyttä, arvioi yhtiön viestintäjohtaja Tuomas Nylund. Koneviat ovat haitanneet tällä viikolla kahden aluksen kulkua Helsingin ja Tukholman välillä.

Matkustaja-autolautta Mariella ajelehti lauantain vastaisena yönä tunnin ajan, koska sähköjärjestelmän häiriö sammutti apukoneet ja niiden mukana pääkoneet.

Gabriella ja sen 1 250 matkustajaa joutuivat keskiviikkona odottamaan Tukholmassa useita tunteja, koska automatiikan häiriö esti pääkoneiden käynnistämisen.

Koneiden sammuminen esti Mariellan ohjaamisen, mutta varageneraattori antoi sähköä

Tonneittain rikkidioksidia pääsi ilmaan

PORVOO. Neste Oilin Porvoonjalostamolta pääsi keskiviikkoaamuna ilmaan 13 tonnia rikkidioksidia. Porvoolaisille päästö ilmeni hajuhaittana.

–Se tuntuu nenässä ja limakalvoilla. Kyllä se kaupungilla huomattiin, kun aamulla ei paljoa tuullutkaan, osastopäällikkö **Sakari Sumela** sanoi.

Sumelan mukaan pitoisuudet ovat niin pienet, että varsinaisia terveyshaittoja ei pitäisi syntyä.

–Astmaatikot sen ovat varmaan kaikkein ärsyttävimpänä tunteneet, hän tuumi.

Päästö johtui automaatiokorttiviasta rikin talteenottoyksikössä. Häiriö alkoi kello viideltä. Se saatiin korjattua kahdeksalta, mutta jonkin verran päästöjä syntyi puoli kymmeneen asti, ennen kuin yksikkö saatiin käyntiin.

Keskiviikkoaamun kaltainen tilanne ei ole Neste Oilin Porvoon jalostamolla kovin yleinen.

–Korttivikoja tulee, mutta harvoin ne näkyvät tässä laajuudessa, Sumela kertoi. **STT**

10.10.2010

Ei-toivotut tapahtumat

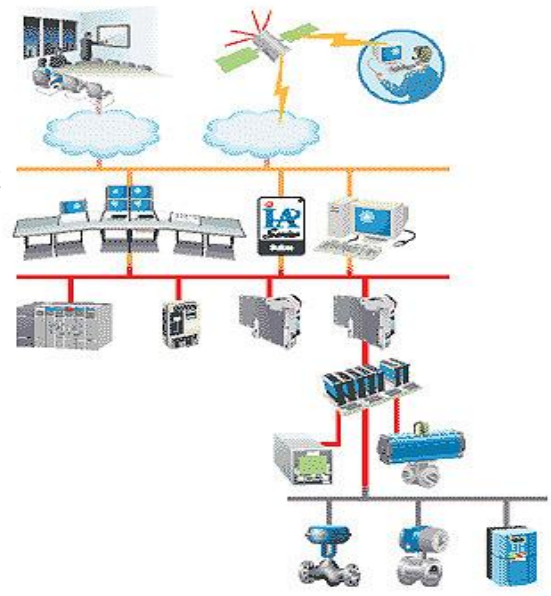
Vahingot:

- ihmisille (eläimille).
- omaisuudelle.
- ympäristölle.
- liiketoiminnalle
  - tuotteille
  - tuotannolle.

Standardi IEC 61508 sopii näiden kaikkien vahinkojen ennalta ehkäisyyn.

10.10.2010

Teollisuusautomaatio-järjestelmän tasot



Teollisuus-ethernet

Kenttäväylät

Anturi/laiteväylät

HS 2.10.2010

Iran ilmoitti sunnuntaina, että tietokonevirus levisi myös Bushehrin ydinvoimalaan.

VIIME kesänä löydetyn Stuxnet-madon alkuperää on arvailtu viime viikkoina useilla teknologiasivustoilla ja kansainvälisessä mediassa. USB-muistitikkujen välityksellä leviävä virus on niin monimutkainen, että asiantuntijoiden mukaan sen kehittämiseen tarvitaan valtion voimavaroja.

Tietoturvayhtiö Symantecin mukaan Stuxnet on luotu iskemään teollisuuslaitoksia ohjaaviin hallintajärjestelmiin, ja sen todennäköisin kohde on Iran. Virus iskee erityisesti Siemens-yhtiön laitteisiin, joita käytetään esimerkiksi öljyputkistojen, sähköverkkojen ja ydinvoimaloiden hallinnassa.

F-Securen blogin mukaan mato voisi teoriassa pysäyttää tuotantolaitoksen tai pahimmassa tapauksessa jopa aiheuttaa räjähdyksen.

Iran ilmoitti sunnuntaina, että virus on levinnyt maan ensimmäiseen ydinvoimalaan Bushehrissa.

Uusia turvallisuusongelmia

- Turvallisuuteen liittyvät ohjelmistot (testaukset)
- Verkottuminen (järjestelmien yhteensopivuus, tietoturvauhkat)
- Tietoliikenteen luotettavuus (kenttä- ja turvaväylät)
- Langaton ohjaus (etäohjaus)
- Iihminen-kone vuorovaikutus (valvomot).

IEC:n ohjausjärjestelmästandardeja

- IEC/CENELEC:

  IEC 61508 1…7 ”kattostandardi” toiminnallisesta turvallisuudesta (ei yhdenmukaistettu)

  IEC 61511 1..3 sovellusstandardi prosessiteollisuudelle

  IEC 62061 sovellusstandardi koneille (yhdenmukaistettu)

  IEC 60204-1 sähkölaitestandardi, yhdenmukaistettu.

Standardoinnin edut

- Yhdenmukaisten käsitteiden käyttö vähentää väärinkäsityksiä ja karkeita virheitä, jotka voisivat olla etenkin toiminnallisen turvallisuuden ja luotettavuuden varmistamisen kannalta katastrofaalisia
- Dokumenttien laadinta helpottuu, mikä on ensiarvoista toiminnallisen turvallisuuden käytönaikaiseen varmistamiseen ja muutostöihin
- Yhdenmukaisten menetelmien käyttö lisää eri sovellusten vertailukelpoisuutta
- Vaatimustenmukaisuuden varmistaminen helpottuu niin asiakkaiden kuin viranomaistenkin suuntaan.

Standardien käyttö

- Standardeissa esitetään suunnitteluperiaatteita ja -menetelmiä sekä ja velvoittavia vaatimuksia (”shall”). Ohjeet ja esimerkit on opastavia ja tarkoitettu standardin vaatimusten ymmärtämiseen (”should”).
- Standardit ovat juridisesti vapaaehtoisesti noudatettavia dokumentteja erotuksena pakottavista säädöksistä (esim. direktiiveistä)
- Eurooppalaiset yhdenmukaistetut standardit antavat ”vaatimustenmukaisuusolettaman” eli standardin vaatimukset täyttävät ratkaisut ovat riittäviä myös lakisääteisten vaatimusten täyttämiseen.
- Standardit tukevat omaa osaamista, mutta eivät sitä korvaa.

Perusstandardi IEC 61508

- ”Kattostandardi” turvallisuuteen liittyvien teknisten järjestelmien (TLJ) sähköisten/elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien turvallisuuden suunnitteluun.
- Soveltamisalaan kuuluvat kaikki sektorit ja sen avulla kehitetään sovellusstandardeja eri sektoreille ja myös laitteille: prosessit, rautatiet, lääkintälaitteet, koneet, taajuusmuuttajat jne.
- Järjestelmällinen lähestymistapa (”Systems Approach”) kaikkiin järjestelmän turvallisuuselinkaaren vaiheisiin.

Perusstandardi IEC 61508

- ”Kattostandardi” IEC 61508 velvoittaa muut standardointielimet ottamaan sen periaatteet , vaatimukset ja menetelmät huomioon uusien standardien valmistelussa ja vanhojen päivittämisessä
- Standardia IEC 61508 käytetään myös sellaisenaan esimerkiksi jos:
  - ei ole sovellusstandardia tai sellaista ei voida soveltaa
  - standardin soveltamisalaan kuuluvien komponenttien ja alajärjestelmien valmistukseen kaikilla sektoreilla (esim. anturit, logiikat jne)
  - vaatimustenmukaisuuteen ja sertifiointiin liittyvän arvioinnin perustana.

IEC 61508 osat 1 ja 2

- Osassa 1 esitetään:
  - yleiset vaatimukset
  - vaatimukset ohjausjärjestelmän vuorovaikutuksesta turvallisuuteen liittyvään prosessiin (tehdas, liikenneväline, koneyhdistelmä).
- Osassa 2 esitetään
  - ohjausjärjestelmän liittäminen ohjattavaan järjestelmään (laitteet, ohjelmistot)
  - laitteet (HW), esimerkiksi vaarallisten satunnaisvikaantumisten taajuus

IEC 61508 osat

- Osassa 3 esitetään ohjelmistovaatimukset.
- Osassa 4 esitetään käsitteet.
- Osassa 5 (opastava) esitetään riskin arvioinnin menetelmiä.
- Osassa 6 (opastava) esitetään ohjeita osien 1...3 soveltamisesta.
- Osassa 7 (opastava) esitetään menetelmiä ja työkaluja.

Toiminnallisen turvallisuuden hallinta

- Turvallisuus yhdistettävä saumattomasti muihin toimintoihin ja se on otettava huomioon heti suunnittelun alussa.
- Laatujärjestelmä (välttämätön)
- Projektinhallinta ja turvallisuussuunnitelma (Safety Plan)
- Turvallisuuden elinkaaritarkastelu ja turvallisuusjohtaminen koko elinkaaren ajan.

Järjestelmällinen lähestymistapa (ohjelmistot)

- Rakenteinen (puolustuksellinen) ohjelmointi (esim. V-malli)
- Moduulirakenne ja yhteensopivuus:
  - testatut (sertifioidut) komponentit ja ohjelmistomoduulit (COTS, toimilohkokirjastot)
  - rajapintojen määritykset (standardit: mm. laitekuvaukset, protokollat jne.).
- Dokumentaation hallinta.

Toiminnallisen turvallisuuden saavuttaminen

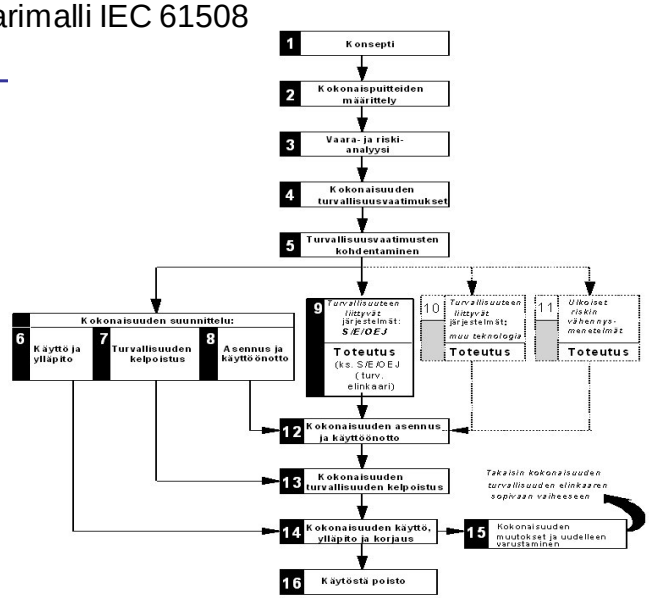
Toiminnallisen turvallisuuden saavuttaminen:

- toiminnallisen turvallisuuden hallinta
- tekniset vaatimukset sovellettavan elinkaaren eri vaiheissa (liite B)
- toiminnallisen turvallisuuden arviointi (FSA)
- henkilöstön pätevyys.

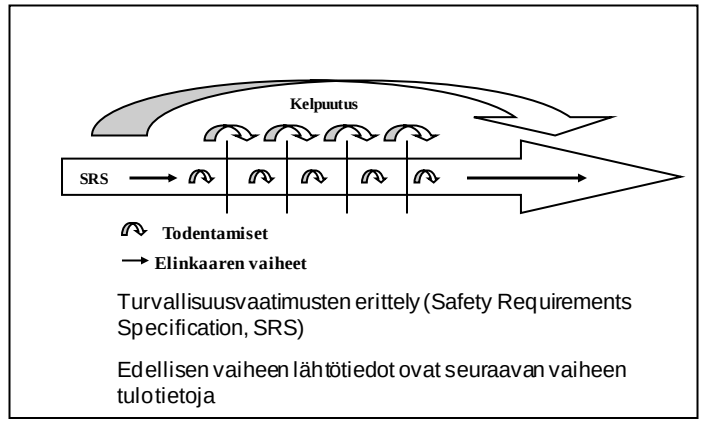
Sovellettavat elinkaarimallit:

- Overall Safety Lifecycle (kuva B.1)
- E/E/PES System Safety Lifecycle (kuva B.2)
- Software Safety Lifecycle (kuva B.3).

Elinkaarimalli IEC 61508



Todentaminen ja kelpuutus

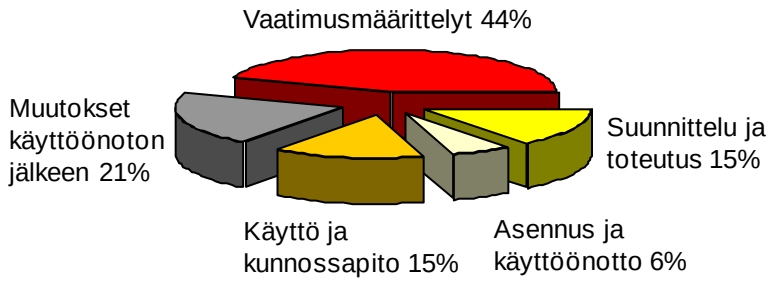


Turvallisuusvaatimusten erittely (Safety Requirements Specification, SRS)

Edellisen vaiheen lähtötiedot ovat seuraavan vaiheen tulotietoja

10.10.2010

Vahinkojen ja onnettomuuksien syitä (prosessiteollisuus)



Automaatio yksin on harvoin onnettomuuden syynä, inhimillinen tekijä on mukana!

10.10.2010

Vaatimusten erittely (esimerkki)

Liikennevälineen elektronisen ohjausyksikön vaatimukset (vanha standardi, SIL 3)

- IEC 61508 osien 1…3 vaatimukset:
  - 378 velvoittavaa vaatimusta (shall)
  - 141 korkealla suositustasolla (should, highly recommended, HR).
- Vaatimusten jakautuminen:
  - osa1 (yleistä) 126 vaatimusta
  - osa 2 (järjestelmä ja laitteet) 194 vaatimusta
  - osa 3 (ohjelmisto) 199 vaatimusta

(Glöe)

Vaatimusten luokittelu

- Vaatimukset valmistajille laadun hallinnasta.
- Elektroniikan toiminnalliset vaatimukset.
- Muut kuin toiminnalliset vaatimukset.
- Vaatimukset valmistajalle todentamisesta ja kelpuutuksesta.
- Vaatimukset kolmannen osapuolen käyttämisestä todentamiseen ja kelpuutukseen.

Dokumentaatio

- Ohjausjärjestelmän suunnittelijan olisi erotettava käyttäjälle merkityksellinen dokumentaatio turvallisuuden suunnitteluun liittyvästä dokumentaatiosta.
- Dokumentaation on oltava
  - tarkka ja täydellinen (jäljitettävyys)
  - dokumentaation käyttäjien helppo ymmärtää (kuvaukset, termit ja kommentit)
  - käyttötarkoitukseen soveltuvaa
  - käytettävissä ja ylläpidettävissä.
- Version hallinnan on oltava kunnossa.
- Tuotetiedon hallintajärjestelmät (digitaalinen tehdas).

Mitä uutta standardeissa IEC 61508-1, -4 ja -5?

- IEC 61508-1: (yleistä): vain pieniä toimituksellisia muutoksia.
- IEC 61508-4 (termit ja käsitteet): termejä ja käsitteitä on täsmennetty ja useita aivan uusia käsitteitä (Jouko Järvi esittelee).
- IEC 61508-5 (riskin arviointi):
  - huomautus siitä, että standardissa ei anneta valmiita turvallisuuden eheyden tasoja (vain menetelmiä ja esimerkkejä)
  - arvioinnin perustana on suhteellisen monimutkainen järjestelmä
  - uudet käsitteet (komponenteille ”Systematic capability” etc.)
  - siedettävän riskin (Tolerable risk) määrittämisessä on otettava huomioon lakisääteiset vaatimukset, käyttäjäorganisaation ohjeet jne.

Mitä uutta standardissa IEC 61508-5? (jatkuu)

- uudet kohdat A.1 ”Henkilökohtainen riski”, A.2 ”Sosiaalinen riski” ja A.3 ”Jatkuva parantaminen” ja A.4 ”Riski profiili”.
- kohdassa A.5 erotellaan harvojen, tiheiden ja jatkuvien vaateiden tapaukset
- lisätty kohdat A 5.2 ja A 5.3 tiheille ja jatkuvien vaateiden tapauksille
- uusi kohta 5.4 ”Yhteisvikaantumiset ja ehdolliset vikaantumiset”
- uusi kohta 5.5 ”Turvallisuuden eheyden tasot kun käytetään useita suojauskerroksia”
- uusi kohta A.9 ”Riskiä lieventävät (mitigating) järjestelmät”
- uusi luku B ”Menetelmien valinta turvallisuuden eheyden tason valintaan”
- uusi luku E.3 ”Kalibrointi” riskigraafin yhteydessä
- uusi taulukko E.2 riskigraafin kalibrointiin
- liite F ”LOPA” kirjoitettu kokonaan uudelleen.

Toiminnallinen turvallisuus

Toiminnallinen turvallisuus on se kokonaisturvallisuuden osa, joka liittyy ohjelmoitavaan järjestelmään ja riippuu sähköisen/elektronisen/ohjelmoitavan elektronisen turvallisuuteen liittyvien järjestelmien, muun teknologian turvallisuuteen liittyvien järjestelmien ja ulkoisten riskin vähennysmenetelmien oikeasta toiminnasta (IEC 61508-5, 3.1.9).

Turvallisuuden eheys SIL (Safety Integrity Level)

Todennäköisyys sille, että turvallisuuteen liittyvä järjestelmä toteuttaa hyväksyttävästi vaadittavat turvatoiminnat kaikissa määritellyissä olosuhteissa ja määriteltynä ajanjaksona.

”Turvatoiminnon luotettavuus”

SIL 1…4 tasot on määritelty kvantitatiivisesti eli kuinka usein korkeintaan turvatoiminnon saa menettää kun sitä tarvitaan (= vaade).

Turvatoiminnot ja vaadetaajudet

Kone tai laite:

- lievät tapaturmat vs. vakavat ja kuolemaanjohtaneet tapaturmat
- käyttö- ja turvatoimintoja ei aina voi erotella (jatkuvien vaateiden toimintamuoto).

Prosessit:

- seurausanalyysit (esim. lukuisia altistuneita, kemikaalipäästön leviäminen)
- käyttö- ja turvajärjestelmät toistaan erotetut (harvojen vaateiden toimintamuoto).

Tiheiden tai jatkuvien vaateiden toimintatapa

- Tiheiden tai jatkuvien vaateiden toimintatapa on kyseessä kun vaade turvatoiminnolle tulee useammin kuin kerran vuodessa tai jatkuvasti
- Turvatoiminnon epäonnistumisen todennäköisyyttä mitataan käsitteellä PFH_d (Probability of Dangerous Failure/hour) , joka on myös vikatajuus λ (Failure Rate) seuraavasti:

  $PFH_d = \lambda$ [1/h].

Turvallisuuden eheyden tasot

Tiheiden vaateiden tai jatkuvan toiminnan toimintatapa.
Vaarallisen vikaantumisen todennäköisyys tuntia kohden PFH_d:

SIL = 4	10^{-9} … 10^{-8} (ei tavallisesti konesovelluksissa)
SIL = 3	10^{-8} … 10^{-7}
SIL = 2	10^{-7} … 10^{-6}
SIL = 1	10^{-6} … 10^{-5} .

Harvojen vaateiden toimintatapa

- Harvojen vaateiden toimintatapa on kysessä kun vaade turvatoiminnolle tulee harvemmin kuin kerran vuodessa
- Turvatoiminnon onnistumisen todennäköisyyttä mitataan käsitteellä PFD (Probability of Failure on Demand)
- Prosessiteollisuudessa käytetään 95 %:sti PFD:tä.

Turvallisuuden eheyden tasot

Turvallisuuden eheydentasot: vaadittavat vikaantumisen enimmäisarvot turvatoiminnolle harvojen vaateiden tapauksessa PFD.

Keskimääräinen vaarallisen vikaantumisen todennäköisyys PFD_{avg} turvatoimintoa vaadittaessa:

SIL 4: $\geq 10^{-5} \ldots < 10^{-4}$
SIL 3: $\geq 10^{-4} \ldots < 10^{-3}$
SIL 2: $\geq 10^{-3} \ldots < 10^{-2}$
SIL 1: $\geq 10^{-2} \ldots < 10^{-1}$

Tietoja standardeista

- Säädökset: www.finlex.fi
- Suomen standardisoimisliitto:
  - www.sfs.fi
  - luettelo standardeista.
- Suomen sähköteknillinen standardisoimisyhdistys SESKO ry (SFS:n toimialayhteisö)
  - www.sesko.fi
  - tietoa sähköturvallisuusstandardeista.
- Metsta ry (SFS:n toimialayhteisö):
  - www.metsta.fi
  - koneturvallisuuden verkkojulkaisu.

Tietolähteitä

- Seskon komitea SK 65 ”Teollisuusprosessien ohjaus”. www.sesko.fi
- Komitean SK 65 kohdealueena on teollisuusprosessien mittaus ja ohjaus. Seskon SK 65 on IEC TC65:n ja CENELEC TC65:n vastinkomitea Suomessa.
- IEC (International Electrotechnical Commission)
  - kansainväliset sähköalan standardit
  - Functional Safety Zone.