Teollisuusautomaation standardit
Osio 3

Osio 1:	SESKOn Komitea SK 65: Teollisuusprosessien ohjaus
Osio 2:	Toiminnallinen turvallisuus: periaatteet
Osio 3:	**Toiminnallinen turvallisuus: standardisarja IEC 61508**
Osio 4:	Koneiden ohjausjärjestelmät: standardi IEC 62061
Osio 5:	Riskin arviointi ja turvallisuuden eheyden tason SIL määrittäminen: standardit IEC 61508-5 ja IEC 62061
Osio 6:	Koneiden ohjausjärjestelmien suunnittelutyökalu SISTEMA
Osio 7:	Hätäpysäytys: standardit ISO 13850 ja IEC 60947-5-5
Osio 8:	Turvaväylät ja niiden valinta: tekninen raportti IEC/TR 62513
Osio 9:	Logiikat: standardi IEC 61131-1 ja 61131-3
Osio 10:	Turvallisuuteen liittyvän elektroniikan asennus- ja muutostyöt

matti.sundquist@sundcon.fi

Toiminnallinen turvallisuus: standardisarja IEC 61508

Matti Sundquist
Sundcon Oy

Standardisarjan IEC 61508 laajan käytön perusteet

- Standardisarjassa IEC 61508 esitetään yksityiskohtaiset vaatimukset toiminnallisesta turvallisuudesta kaikille teknisille järjestelmille.
- Standardissa esitetään ohjeita ja ratkaisuesimerkkejä siitä, miten turvallisuuteen liittyvä automaatiojärjestelmä suunnitellaan, toteutetaan, testataan, otetaan käyttöön ja miten sen muutokset hallitaan.
- Standardi esittää yksityiskohtaisesti, mitä edellytetään tietyn turvallisuuden eheyden tason saavuttamiseksi ja esittää siihen vaihtoehtoja.

Standardisarjan IEC 61508 käytön etuja

- Standardin IEC 61508 avulla automaatiojärjestelmän vaatimustenmukaisuus on helpompi osoittaa, koska teollisuus ja viranomaiset käyttävät sitä referenssinä.
- Standardia käytetään teknisenä laatumäärittelynä ja standardiviittaus kattaa useita satoja vaatimuksia.
- Globaalisti toimivat yritykset (sekä käyttäjät että prosessi-/laitevalmistajat) haluavat sen vähitellen korvaavan vastaavat kansalliset standardit.

Perusstandardi IEC 61508

- Standardi IEC 61508 on perusstandardi (”kattostandardi”) koskee kaikkien turvallisuuteen liittyvien teknisten järjestelmien (TLJ) suunnittelua ja toteutusta, joissa käytetään sähköistä/elektronisia ja ohjelmoitavia elektronisia ohjausjärjestelmiä.
- Sen soveltamisstandardeja on laadittu mm.: prosessiteollisuuteen, koneille, rautateille, voimalaitoksille, lääkintälaitteille jne.

IEC 61508 – Turvallisuuden kattostandardi

IEC EN 61508

- EN IEC 61511: Prosessiteollisuus
- EN IEC 61513, 62138: Ydinvoimalat (EN IEC 61226)
- EN IEC 62061: Koneet ja laitteet
- EN IEC 61131-x: (Turva)logiikat

EN 50128: Rautatiet

SFS-EN ISO13849-1 (korvaa ISO 13849-1:2003 ja EN 954)

Perusstandardi IEC 61508

- Perusstandardi IEC 61508 velvoittaa muut standardointielimet ottamaan sen periaatteet, vaatimukset ja menetelmät huomioon uusien standardien valmistelussa ja vanhojen päivittämisessä.

Perusstandardi IEC 61508

- Standardia IEC 61508 käytetään myös sellaisenaan, esimerkiksi jos ei ole sovellusstandardia tai sellaista ei voida soveltaa.
- Siten standardia IEC 61508 sovelletaan muun muassa sen soveltamisalaan kuuluvien komponenttien ja alajärjestelmien valmistukseen (esim. anturit, logiikat jne.) tai sitä käytetään vaatimustenmukaisuuteen ja sertifiointiin liittyvän arvioinnin perustana.

IEC 61508 osat 1 ja 2

- Osassa 1 esitetään yleiset vaatimukset, mm. vaatimukset ohjausjärjestelmän vuorovaikutuksesta turvallisuuteen liittyvän prosessin kanssa, esim. tehdas, liikenneväline, koneyhdistelmä.
- Osassa 2 esitetään ohjausjärjestelmän liittäminen ohjattavaan järjestelmään (laitteistot, ohjelmistot), esimerkiksi turvatoimintoa toteuttavan järjestelmän vaarallisten satunnaisvikaantumisten suurin 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.

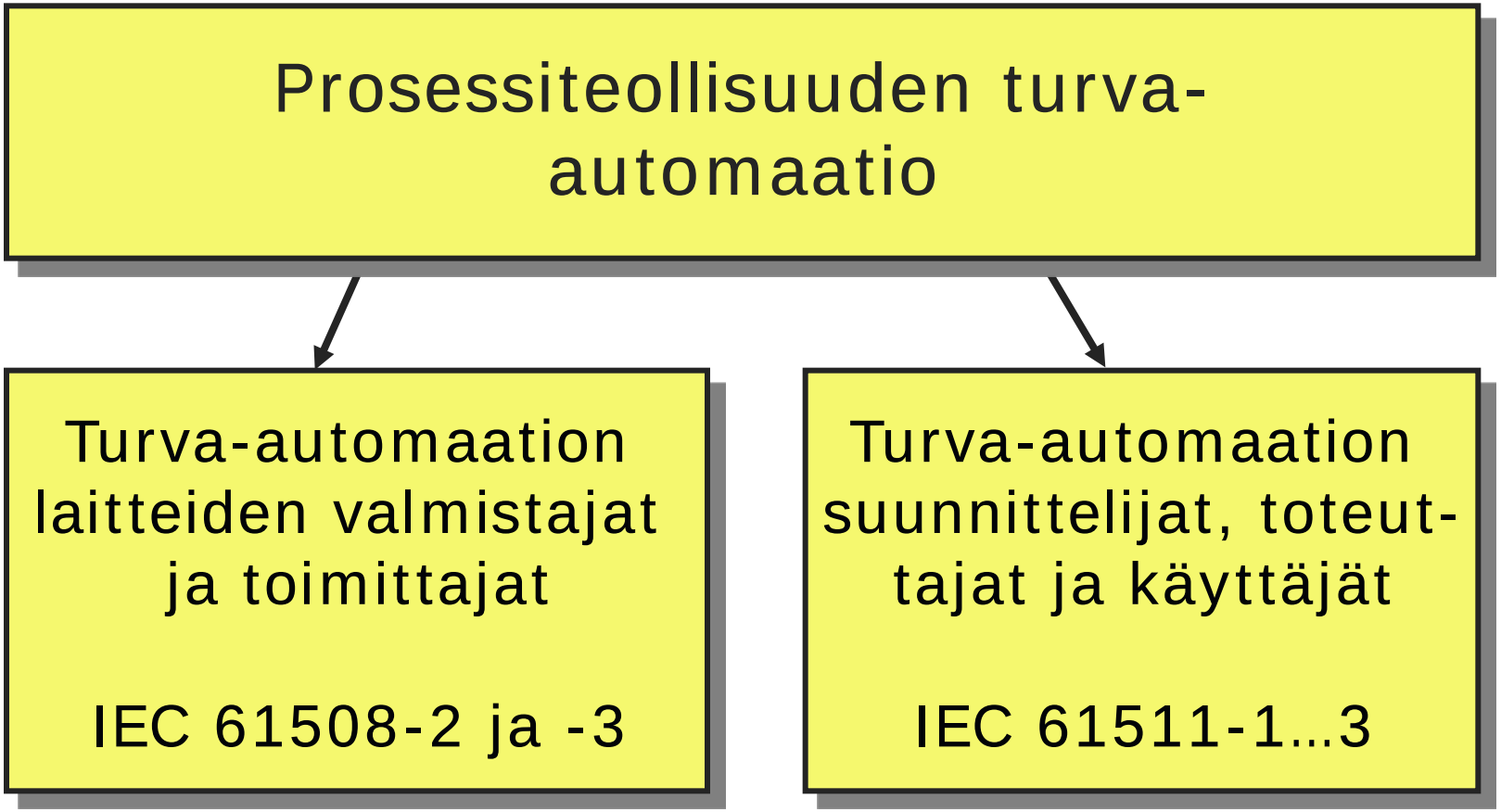
Turvallisuuden hallinnan lähtökohta

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

Standardisarjan IEC 61508 sovellusalueita

- Prosessien ja koneiden ohjaus
- Koneiden ohjaus ja turvalaitteet
- Vesi- ja jätevesijärjestelmät
- Ydinvoimaloiden ja muiden voimalaitosten automaatio
- Rautatiejärjestelmien ohjaus
- Ajoneuvojen sulautettu ohjaus
- Kaivosteollisuuden laitteet
- Hissien ohjaus.

IEC 61508 ja IEC 61511 osien käyttäjiä



IEC 61508 peruskonsepti

- Turvallisuuden elinkaari
- Tarkat yksilöidyt suunnittelu-menetelmät
- Systemaattiset viat ja suunnitteluvirheet

Ohjelmistokehitys

- Todennäköiseen suorituskykyyn perustuva järjestelmä
- Satunnais-vikaantumiset

Laitteiston suunnittelu

Sertifioidut komponentit

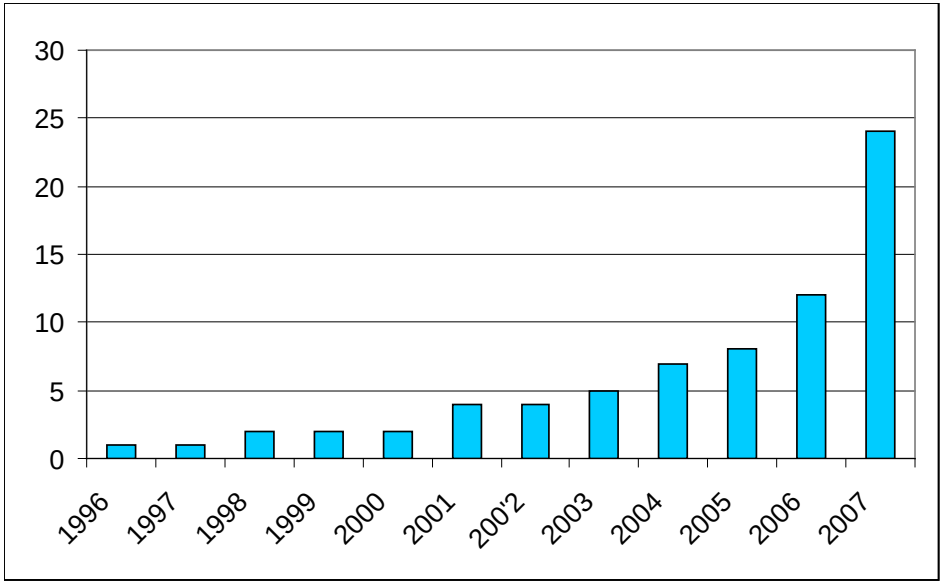
- Komponenttien sertifioinnilla tarkoitetaan riippumattoman osapuolen tekemää arviointia siitä, että tuote täyttää sitä koskevat vaatimukset sekä rakenteen että dokumentaation osalta.
- Nämä vaatimukset voivat olla lakisääteisiä vaatimuksia tai standardien ja muiden erittelyjen vaatimuksia.
- Sertifioinnista annetaan todistus eli sertifikaatti.

Laitteiden IEC 61508-sertifiointi

- Sertifiointi tarkoittaa puolueettoman tahon varmistusta siihen, että laite täyttää sille asetetut vaatimukset.
- Sertifiointi osoittaa hyvää suunnittelutasoa ja sillä perustellaan laitevalintoja.

Sertifioitujen tuotteiden määrä on nopeassa kasvussa. Lähde: Exidan raportti sertifioiduista tuotteista.

IEC 61508 sertifioidut anturit



IEC 61508:n mukainen analyysi turvasertifiointia varten

- Laitteiston suunnitteluprosessin arviointi
- Laitteiston vikaantumistapojen analyysi
- Laitteiston diagnostisten ominaisuuksien analyysi
- Laitteiston luotettavan käyttöiän analyysi
- Ohjelmistovaatimusten arviointi
- Ohjelmiston suunnittelumenetelmien arviointi
- Ohjelmiston testausmenetelmien arviointi
- Konfiguroinnin hallinnan arviointi
- Suunnittelun versiohistorian arviointi
- Käyttökokemusten arviointi
- Toimintatestauksen kattavuuden analyysi
- Turvaohjeistuksen arviointi
- jne.

Lähde: Exida

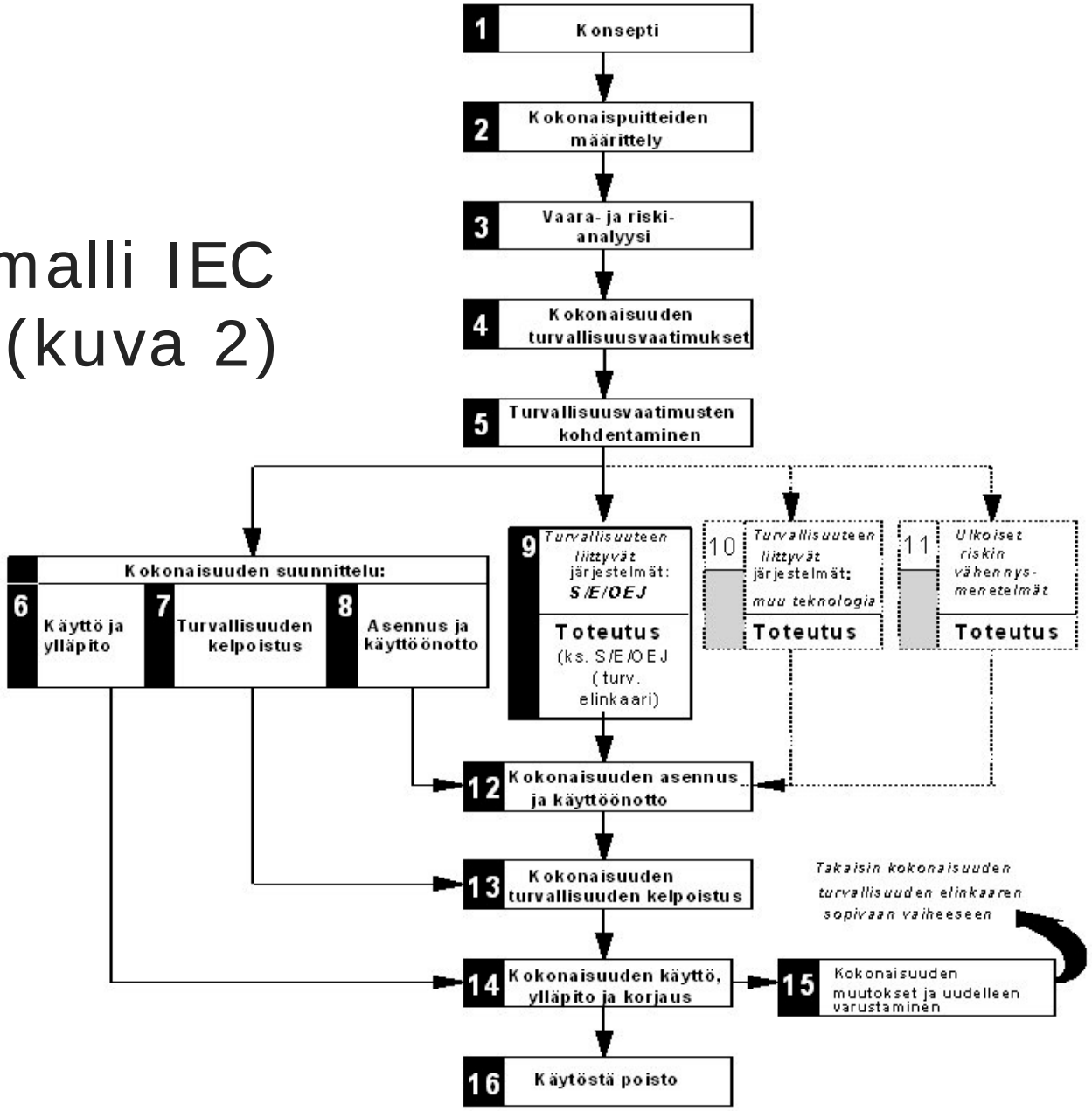
Toiminnallisen turvallisuuden saavuttaminen

- Toiminnallisen turvallisuuden saavuttaminen:
  - toiminnallisen turvallisuuden hallinta
  - henkilöstön pätevyys
  - teknisten vaatimusten täyttäminen elinkaaren eri vaiheissa
  - toiminnallisen turvallisuuden arviointi.
- Sovellettavat elinkaarimallit:
  - Overall Safety Lifecycle (koko järjestelmän elinkaari)
  - E/E/PES System Safety Lifecycle (sähköisen ohjausjärjestelmän elinkaari)
  - Software Safety Lifecycle (ohjelmiston elinkaari).

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.

Elinkaarimalli IEC 61508-1 (kuva 2)



Vaatimusten luokittelu

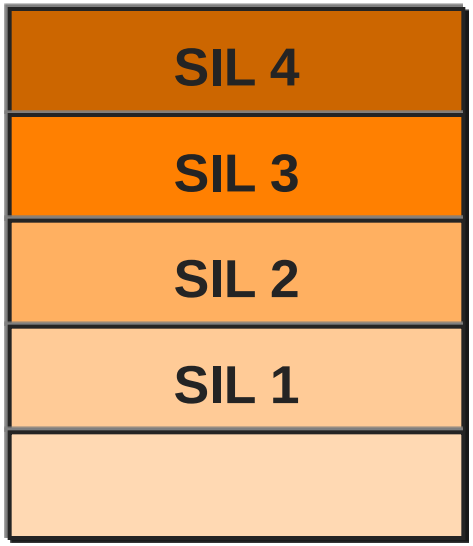
- Vaatimukset valmistajille laadun hallinnasta
- Elektroniikan toiminnalliset vaatimukset
- Muut kuin toiminnalliset vaatimukset
- Vaatimukset valmistajalle todentamisesta ja kelpuutuksesta
- Vaatimukset kolmannen osapuolen käyttämisestä todentamiseen ja kelpuutukseen.

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 satunnaisvikaantumisille eli kuinka usein korkeintaan turvatoiminnon saa menettää kun sitä tarvitaan (= vaade). Myös ohjelmistovaatimukset on luokiteltu SIL-tasojen mukaisesti.

Turvallisuuden eheyden tasojen SIL käyttö

Turvallisuuden eheyden tasoja käytetään seuraavilla tavoilla:



1. Määrittämään vaaran vähentämistarpeet.
2. Asettamaan todennäköiset rajat laitteiden satunnaisvioille.
3. Määrittämään suunnittelu-menetelmät, joilla estetään systemaattiset suunnitteluvirheet (mm. ohjelmistot).

Lähde: W. Goble, Exida

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 toisistaan 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 kyseessä 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

Harvojen vaateiden toimintatapa.
Keskimääräinen vaarallisen vikaantumisen todennäköisyys turvatoimintoa vaadittaessa PFD_{avg}:

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

Dokumentaatio

- Ohjausjärjestelmän suunnittelijan olisi erotettava toisistaan käyttäjälle merkityksellinen dokumentaatio turvallisuuden suunnitteluun liittyvästä dokumentaatiosta
- Dokumentaation on oltava
  - tarkka ja täydellinen (jäljitettävyys)
  - käyttäjien helposti ymmärrettävissä (kuvaukset, termit ja kommentit)
  - käyttötarkoitukseen soveltuvaa
  - käytettävissä ja ylläpidettävissä.
- Versioiden hallinnan on oltava kunnossa.