IEC61508 turvastandardi ja sen merkitys prosessiteollisuudelle

Dr. William M. Goble

exida

Sellersville, PA USA

Martti Hakonen

Emerson Process

Management Oy

Esityksen taustaa

Esitys perustuu Automaatio 2009 seminaaripäivillä 17.3.2009 Bill Goblen pitämiin turva-automaatiota käsitelleisiin esityksiin.

Dr. William M. Goble

exida

Sellersville, PA USA

CFSE

CFSE= Certified Functional Safety Engineer

IEC/EN 61508 – Toiminnallinen turvallisuus

Toiminnallisen turvallisuuden tavoite:

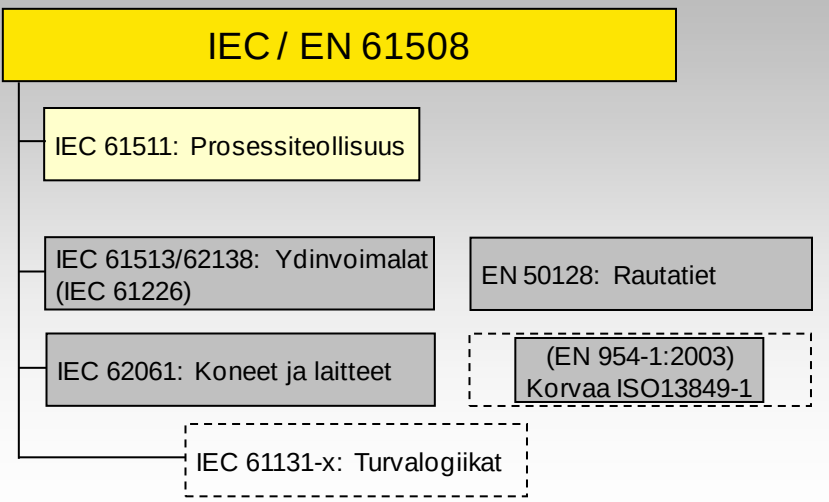
Turvatoiminto suoritetaan suunnitellusti tai sen suorittaminen epäonnistuu ennakoidulla (= turvallisella) tavalla.

IEC 61508 standardia voidaan soveltaa monella tasolla

- **Komponentit**
  - **Prosessien arvioinnit, vika-analyysit/vikatiedot ja dokumentaatio auttamaan tuotteiden kehittämisessä**
- **Tuotteet**
  - **Prosessien arvioinnit, vika-analyysit/vikatiedot ja dokumentaatio (käsittäen mm. turvaohjeen) auttamaan tuotteiden käytössä laitteistojen suunnitteluun**
- **Järjestelmät**
  - **Riskianalyysipohjaiset perusteet SIL-tason ja prosessien arviointiin sekä järjestelmien vikaantumisten analyysit**

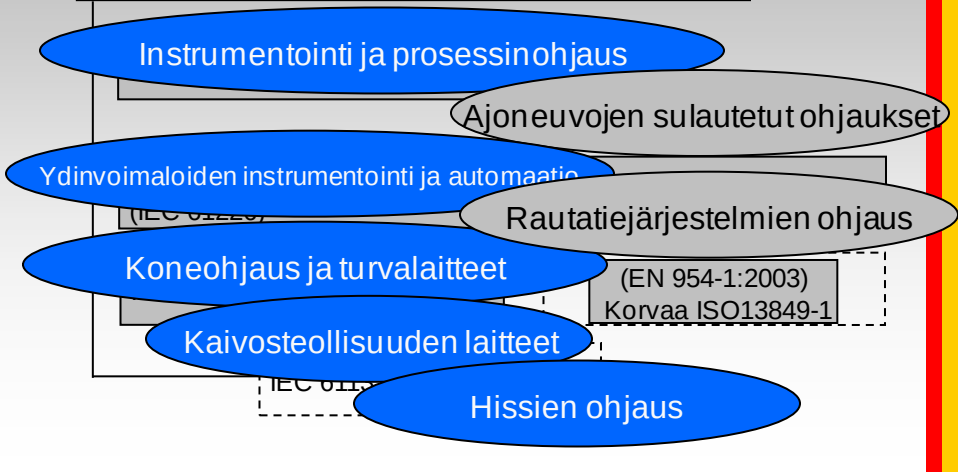
exida

IEC61508 – Turvallisuuden kattostandardi

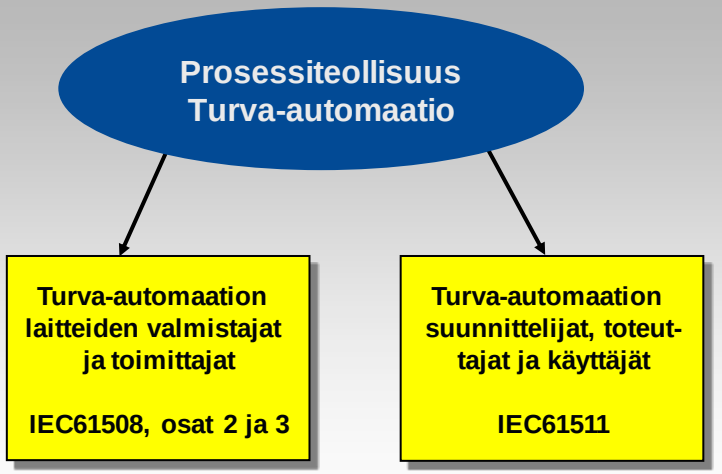


exida

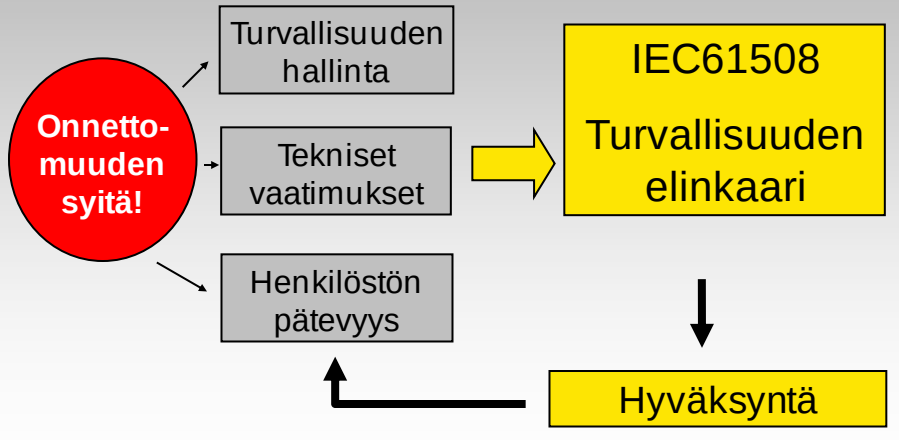
IEC61508 – Nykyinen käyttö



IEC61508 ja IEC61511 kohdealueet



IEC 61508 – Pääkohteet



IEC 61508 – Peruskonsepti

IEC61508 turvallisuuden elinkaari – Tarkat, yksilöidyt suunnittelu-	Todennäköiseen suorituskykyyn perustuva järjestelmäsuunnittelu
Systemaattiset viat – Suunnitteluvirheet	Satunnaisviat
OHJELMISTON VIRHEETTÖMYYS	LAITTEISTON LUOTETTAVUUS

Turvallisuuden eheystaso

SIL

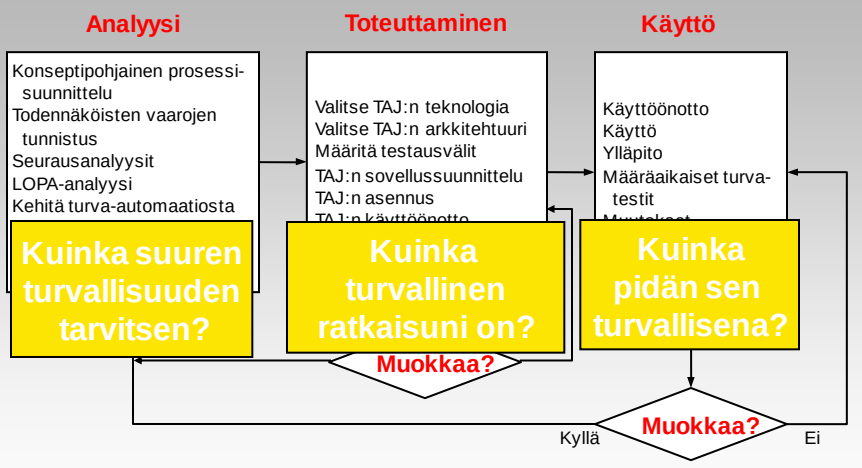
(= Safety Integrity Level)
SIL 4
SIL 3
SIL 2
SIL 1

Käytetään **KOLMELLA** tavalla:

1. Määrittämään vaaran vähentämistarpeet
2. Asettamaan todennäköiset rajat laitteiden satunnaisvioille
3. Määrittämään suunnittelu-menetelmät, joilla estetään systemaattiset suunnittelu-virheet

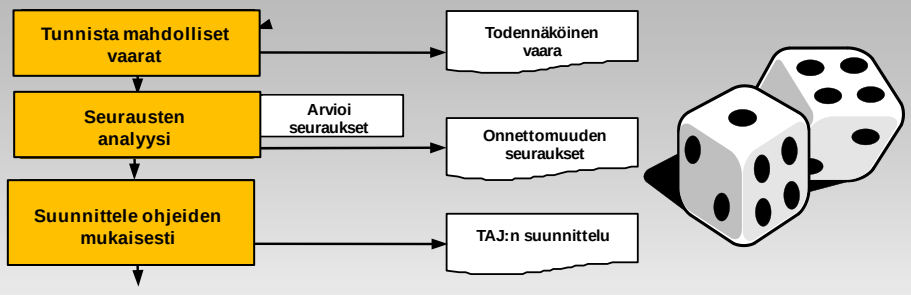
SIL = Safety Integrity Level = Turvallisuuden eheystaso (= TET)

Turvallisuuden elinkaari



LOPA = Layer of Protection Analysis = Suojauskerrosten analyysi
TLJ = Turva-automaatiojärjestelmä = Safety Instrumented Systems (SIS)

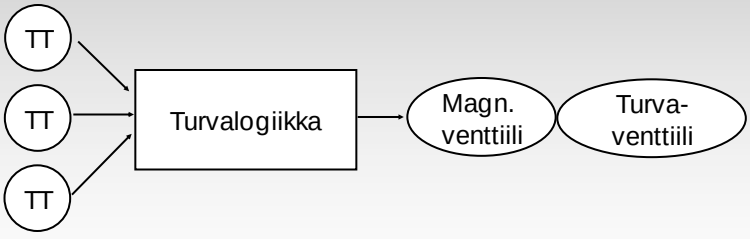
Aikaisempi “elinkaari”



Ehdotus: Säästä kustannuksia verrattuna toteutukseen IEC 61511:n mukaisesti.
Ei toimi! Suunnittelumenettely on puutteellinen mm. elinkaaritarkastelun osalta.

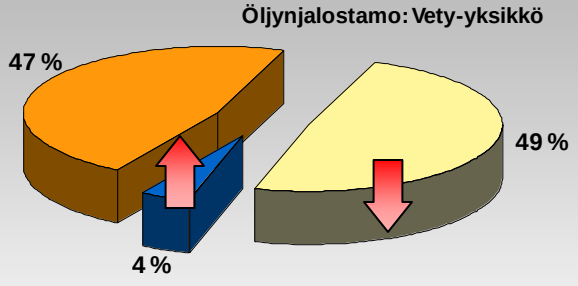
Perinteinen suunnittelumenettely

- **Mikäli turva-automaatiokohde**
  - **Suunnitellaan kolmella lähettimellä, äänestys 2oo3**
  - **Käytetään perinteistä turvalogiikkaa**
  - **Turvatoiminto poistamalla paineilmasyöttö turvaventtiilin toimilaitteelta, käytössä 3-tie magneettiventtiili**



Turva-automaation toteutukset

Käytännön tuloksia turvaratkaisuista

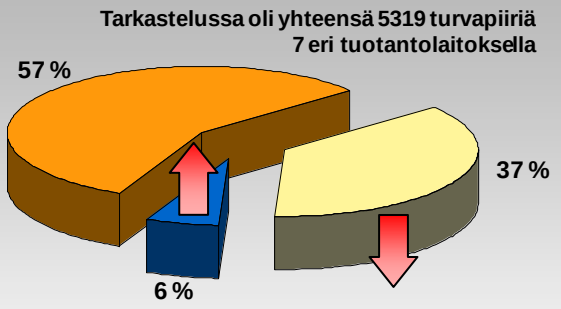


Lähde

- **49%: Turvatoiminnot olivat vaadittua parempia**
- **4%: Turvatoiminnot eivät täyttäneet vaatimustasoa**
- **47%: Ei muutostarvetta**

Turva-automaation toteutukset

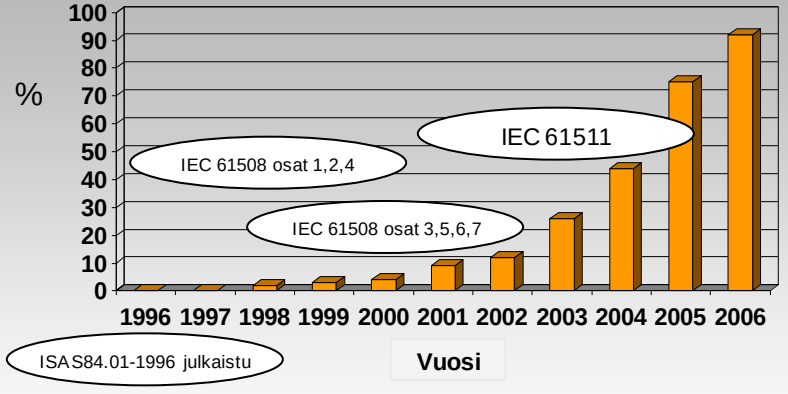
Käytännön tuloksia turvaratkaisuista



Lähde: NAM

- **37%: Turvatoiminnot olivat vaadittua parempia**
- **6%: Turvatoiminnot eivät täyttäneet vaatimustasoa**
- **57%: Ei muutostarvetta**

Turvastandardien käyttö



Onko yrityksesi käyttämässä tai suunnitteleeko käyttävänsä nykyisiä turvastandardeja?

ISA S84.01 on IEC 61508:n edeltäjiä (exida suoritti kyselyn USAssa)

Laitetaso - IEC 61508 sertifiointi


Certificate / Certificat
Zertifikat / 認証
GE 070611 C001
Mark Vies YVIB
Vibration Detection Subsystem
GE Energy
Salem, VA
USA
IEC 61508 Parts 1, 2, 3
Systematic Integrity: SIL 2 Capable
Random Integrity: SIL 1 @ HFT=0, SIL 2 @ HFT=1.
Product Assessor
Auditor
exida Certification S.A.
Page 1 of 2

- Sertifiointiprosessin varmistaa todistus, jossa vahvistetaan, millä SIL-tasoilla laitetta voidaan hyväksytysti käyttää ja luetellaan standardit, joiden mukaisesti sertifiointi on myönnetty.
- Hyvä sertifiointilausunto vahvistaa, että laitteisto ja sen ohjelmisto on hyvin suunniteltu ja sen valmistuslaatu on hyvä.
- Sertifiointiprosessi käsittää myös laitteen mukana käyttäjälle toimitettavan aineiston – eli “turvaohjeen”, jota on noudatettava

IEC 61508 sertifioituja tuotteita

IEC 61508 sertifioituja tuotteita:

Painelähettimet

Lämpötilalähettimet

Virtauslähettimet

Pintalähettimet

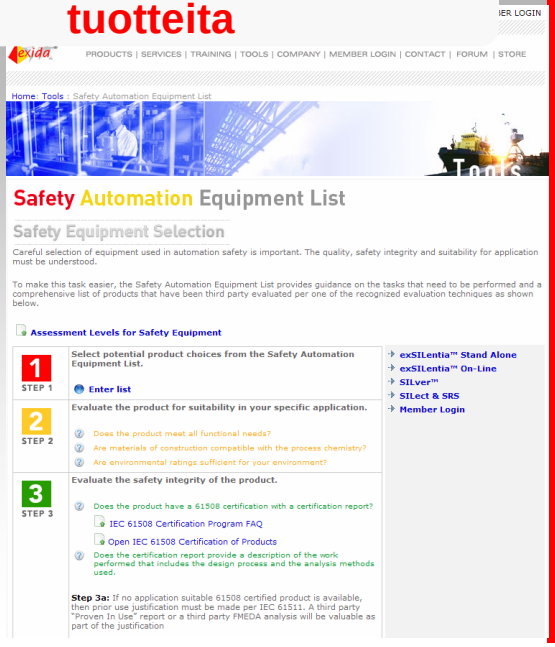
Turvalogiikat

Raja-arvoyksiköt ja modulit

Toimilaitteet

Magneettiventtiilit

Venttiilit



IEC 61508 sertifioituja turvalogii-koita

exida Certification S.A.

Company	Model	Description	Assessment	Assessor	Assessment Report	Contact	Link
ABB	800xA Safety	Safety PLC	61508 Certified	TÜV SÜD			
ABB	Safeguard 400	Safety PLC	61508 Certified	TÜV SÜD			
Emerson Process Automation	DeltaV SIS	Safety PLC	61508 Certified	exida			
GE Energy	Mark Vie	Safety PLC	61508 Certified	exida			
GE Fanuc Automation	GMR	Safety PLC	61508 Certified	TÜV Rh.			
HIMA	H41/H51q	Safety PLC	61508 Certified	TÜV Rh.			
HIMA	A1/A1 dig	Safety PLC	61508 Certified	TÜV Rh.			
Honeywell	FSC	Safety PLC	61508 Certified	TÜV Rh.			
ICS Triplex	Trusted	Safety PLC	61508 Certified	TÜV Rh.			
MTL	safetyNet	Safety PLC	61508 Certified	TÜV Rh.			
Rockwell	ControlLogix	Safety PLC		TÜV Rh			
RTP Corp	2500	Safety PLC	61508 Certified	TÜV SÜD			
Siemens AG	S7-300 F	Safety PLC	61508 Certified	TÜV SÜD			
Siemens AG	S7-400F, S7-400F/H	Safety PLC	61508 Certified	TÜV SÜD			
Triconex	Tricon V9	Safety PLC	61508 Certified	TÜV Rh.			
Triconex	Trident	Safety PLC	61508 Certified	TÜV Rh.			
Yokogawa Electric Corporation	Prosafe-RS	Safety Controller / PLC	61508 Certified	TÜV Rh.			

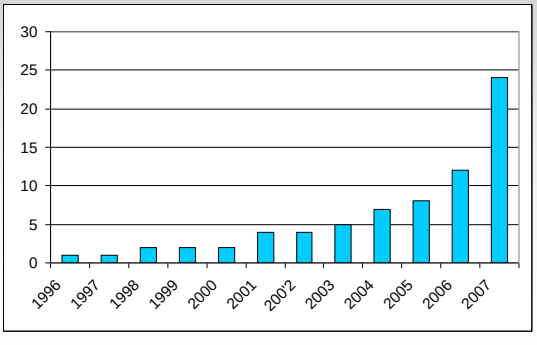
Company	Model	Description	Assessment	Assessor	Assessment Report	Contact	Link
Det-tronics	Eagle Quantum Premier	Fire and Gas Controller	61508 Certified	exida			
Det-tronics	ELS	Fire and Gas Controllers	61508 Certified	TÜV Rh.			
MSA	Suprema	Fire and Gas Controller	61508 Certified	TÜV Rh.			

Huom: Tilanne 3/2009

Suuntaus kohti IEC61508 sertifioituja laitteita

- **IEC 61508 sertifiointi on yksi merkki hyvästä suunnittelutasosta.**
- **IEC 61508 sertifiointi varmistaa perustellun laitevalinnan suppeimmalla tarvittavalla lisädokumentaatiolla.**
- **IEC 61508 sertifioitujen tuotteiden määrä on nopeassa kasvussa:**

Lähde: exidan raportti sertifioiduista tuotteista



IEC 61508 sertifioidut anturit

Terminologiaa:
”Lähetin” on turva-automaatiossa ”anturi”

IEC 61508 sertifioituja paine-lähettimiä

exida Certification S.A.

TÜV NORD

Safety Automation Equipment List

Please Choose Device

IEC61508 CERTIFIED

Company	Model	Description	Assessment	Assessor	Assessment Report	Contact	Link
Endress+Hauser	Cerabar S / Deltabar	Pressure transmitter	61508 Certified	TÜV SÜD			
Honeywell	ST3000	Pressure transmitter	61508 Certified	TÜV Nord			
Rosemount Inc.	3051S SIS	Pressure transmitter	61508 Certified				
Rosemount Inc.	3051 C / T / L	Pressure transmitter, V7.0	61508 Certified				
Yokogawa Electric Corporation	EJX	Pressure transmitter	61508 Certified				

NOT IEC61508 CERTIFIED - PRIOR USE JUSTIFICATION NEEDED

Company	Model	Description	Assessment	Assessor	Assessment Report	Contact	Link
ABB	2600T/2000T	Pressure Transmitter	exida Proven In Use				
Endress+Hauser	Cerabar M	Pressure transmitter	exida Proven in Use				
Endress+Hauser	Cerabar T	Pressure transmitter	Prior-use	TÜV SÜD			

Huom: Tilanne 3/2009

IEC 61508 sertifioituja palloventtii-lejä

Company	Model	Description	Product Evaluation Report	Assessment	Assessor	Assessment Report	Contact	Link
Fisher Controls	V150, V200	Vee-Ball		61508 Certified				
Fisher Controls	V300 Series	Rotary Valves		61508 Certified				
Virgo Engineering	S Series	Ball Valve		61508 Certified				
Virgo Engineering	N Series	Ball Valve		61508 Certified				
MOGAS	C-Series	Severe Service - Seat Metal		FMEDA				
SOMAS Instrument	KVT*/KVX*	Ball Segment Valve		FMEDA				
SOMAS Instrument	SKV	Ball Valve		FMEDA				

Huom: Tilanne 3/2009

exida Certification S.A.

IEC 61508:n mukainen perinpohjainen analyysi turvasertifiointiin, sisältäen mm.:

- 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.

IEC61508 – tuotesertifioinnin esteitä

1. Hardware – täytettävä PFDavg-vaatimus SIL-tavoitetasolle:
   - Vähän vikoja, suunniteltu vikaantumaan turvallisesti
   - Hyvä diagnostiikan kattavuus
2. Hardware – täyttää SFF vaatimuksen SIL-tavoitetasolle
   - Min. SFF 90% SIL2 tasolle
   - Min. SFF 60% SIL1 tasolle
3. **Ohjelmisto – Täyttää vaatimukset SIL-tavoitetasolle, systemaattiset viat on estetty riittävän hyvin**
4. Tuote – Tuotteen suunnitteluprosessi täyttää SIL-tavoitetason vaatimukset, systemaattiset viat on estetty riittävän hyvin
5. Turvaohje varmistamaan laitteen oikean käytön

PFDavg = Probability of Failure on Demand = todennäköisesti epäonnistua vaateen ilmetessä
SFF = Safe Failure Factor = turvallisten vikojen ja vaarallisten havaittujen vikojen yhteismäärä

IEC61508 on laaja ja monimutkainen Miksi sitä käytetään?

Teollisuus ja viranomaiset käyttävät sitä referenssinä pienentämään laajatoimisten toteutusten virheellistä toimintaa

Sitä käytetään teknisenä laatumäärittelynä
(Yksi viittaus kattaa yli 350 vaatimusta)

Globaalisti toimivat yritykset (käyttäjät ja valmistajat) toivovat sen korvaavan kansalliset standardit

IEC61508 on laaja ja monimutkainen Miksi sitä käytetään?

Se antaa vastaukset yksityiskohtaisiin kysymyksiin, mitä todella edellytetään tietyn eheystason saavuttamiseen.

Lisäksi: Se tarjoaa vaihtoehtoja

Kiitos, kysyttävää