

IEC61508 turvastandardi ja sen merkitys prosessiteollisuudelle

Dr. William M. Goble

exida

Sellersville, PA USA

Martti Hakonen

Kunnossapitoyhdistys

Promaint ry

ASAF teemakokous

17.10.2011 Pasila

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

IEC/EN 61508 – Toiminnallinen turvallisuus

Toiminnallisen turvallisuuden tavoite:

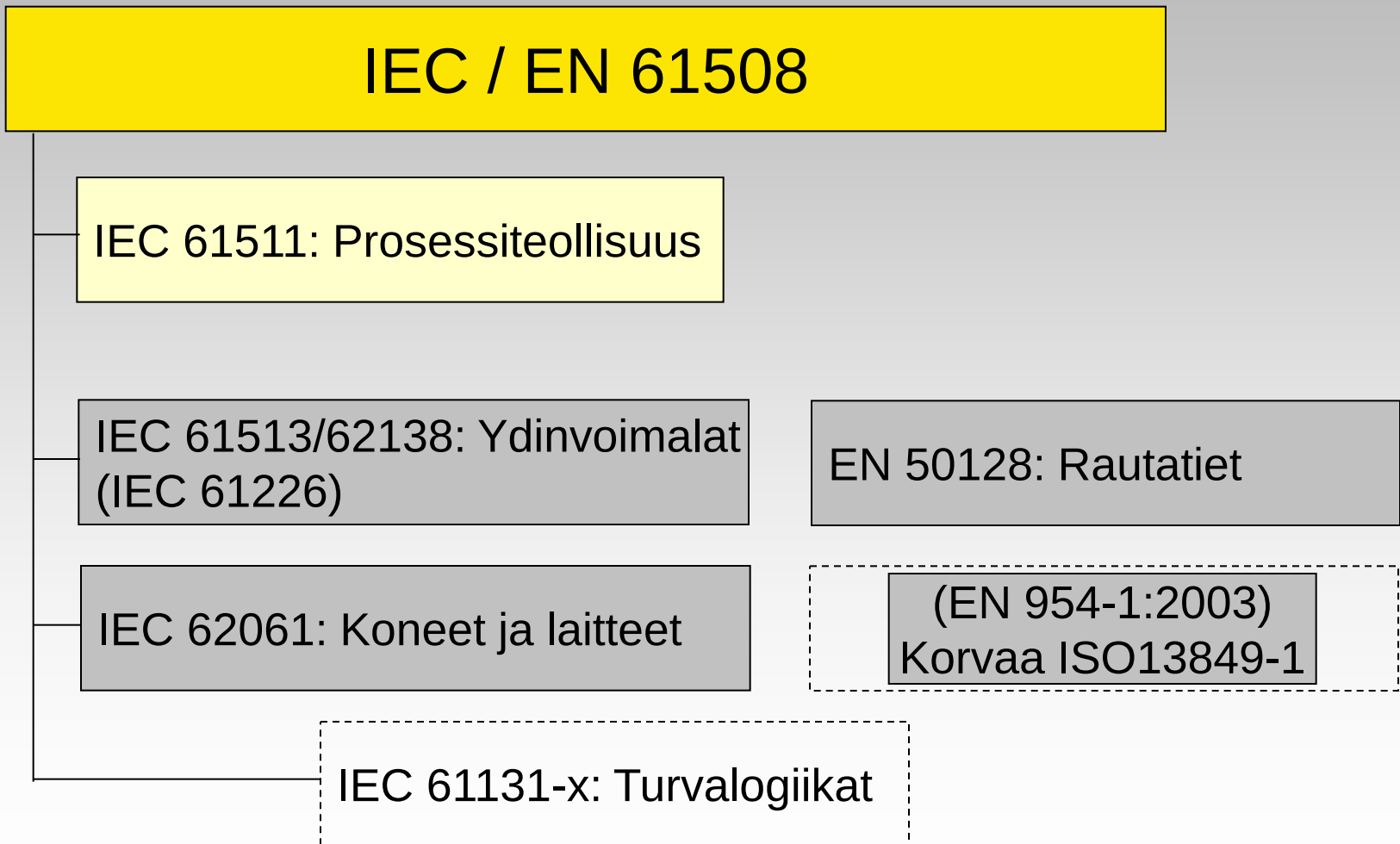
Turvatoiminto suoritetaan
suunnitellusti tai sen suorittaminen
epäonnistuu ennakoidulla
(= turvallisella) tavalla.

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

IEC61508 – Turvallisuuden kattostandardi



IEC61508 – Nykyinen käyttö

IEC / EN 61508

Instrumentointi ja prosessiohjaus

Ajoneuvojen sulautetut ohjaukset

Ydinvoimaloiden instrumentointi ja automaatio

Rautatiejärjestelmien ohjaus

Koneohjaus ja turvalaitteet

(EN 954-1:2003)
Korvaa ISO13849-1

Kaivosteollisuuden laitteet

Hissien ohjaus

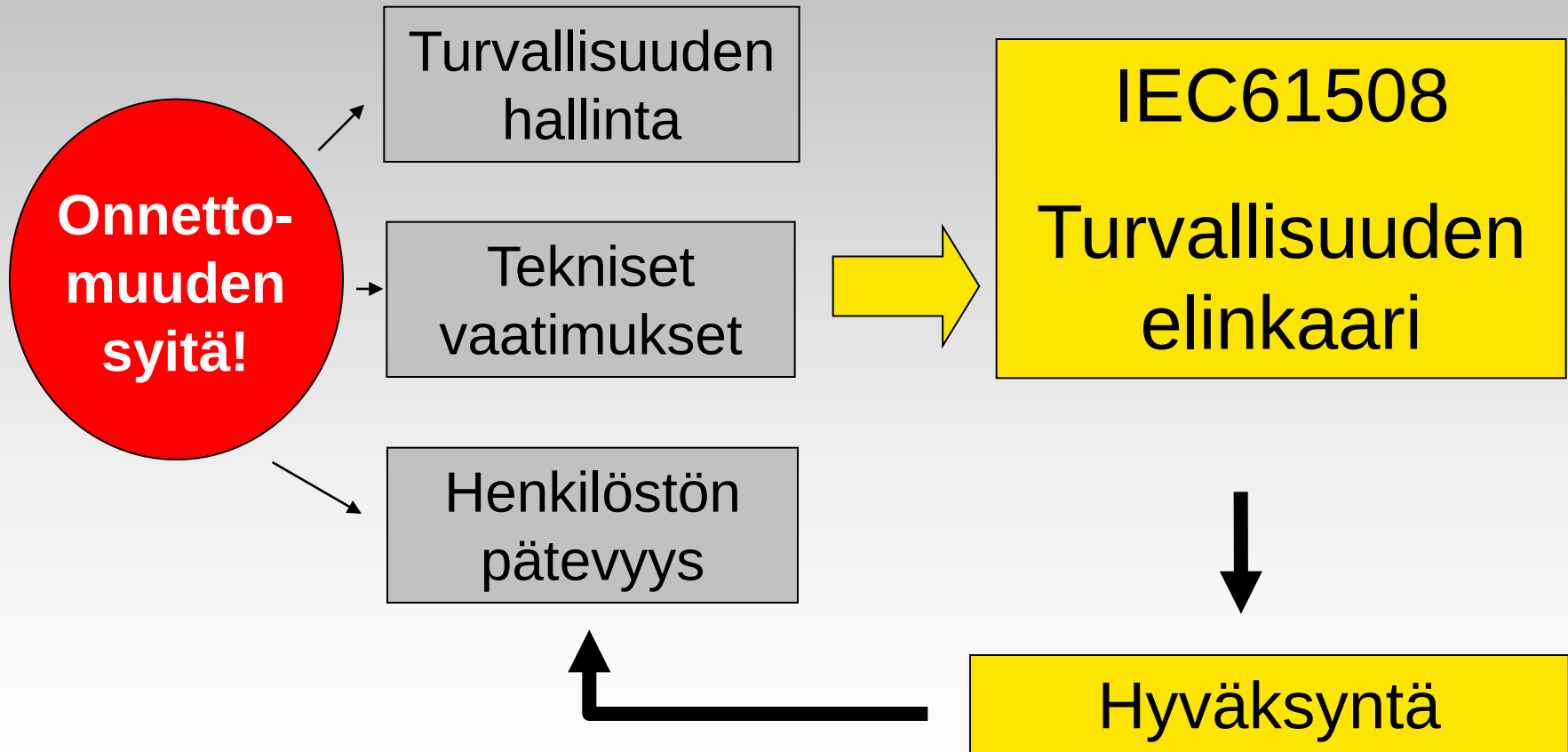
Prosessiteollisuus Turva-automaatio

**Turva-automaation
laitteiden valmistajat
ja toimittajat**

IEC61508, osat 2 ja 3

**Turva-automaation
suunnittelijat, toteut-
tajat ja käyttäjät**

IEC61511



IEC61508 turvalli-
suuden elinkaari –
Tarkat, yksilöidyt
suunnittelu-

Systemaattiset viat
– Suunnitteluvirheet

OHJELMISTON
VIRHEETTÖMYYS

Todennäköiseen
suorituskykyyn
perustuva järjes-
telmäsuunnittelu

Satunnaisviat

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

Turvallisuuden elinkaari

Analyysi

Konseptipohjainen prosessisuunnittelu
 Todennäköisten vaarojen tunnistus
 Seurausanalyysit
 LOPA-analyysi
 Kehitä turva-automaatiosta

Kuinka suuren turvallisuuden tarvitsen?

Toteuttaminen

Valitse TAJ:n teknologia
 Valitse TAJ:n arkkitehtuuri
 Määritä testausvälit
 TAJ:n sovellussuunnittelu
 TAJ:n asennus
 TAJ:n käyttöönotto

Kuinka turvallinen ratkaisuni on?

Muokkaa?

Käyttö

Käyttöönotto
 Käyttö
 Ylläpito
 Määräaikaisten turvatestien suorittaminen
 Muutokset

Kuinka pidän sen turvallisena?

Muokkaa?

Kyllä

Ei

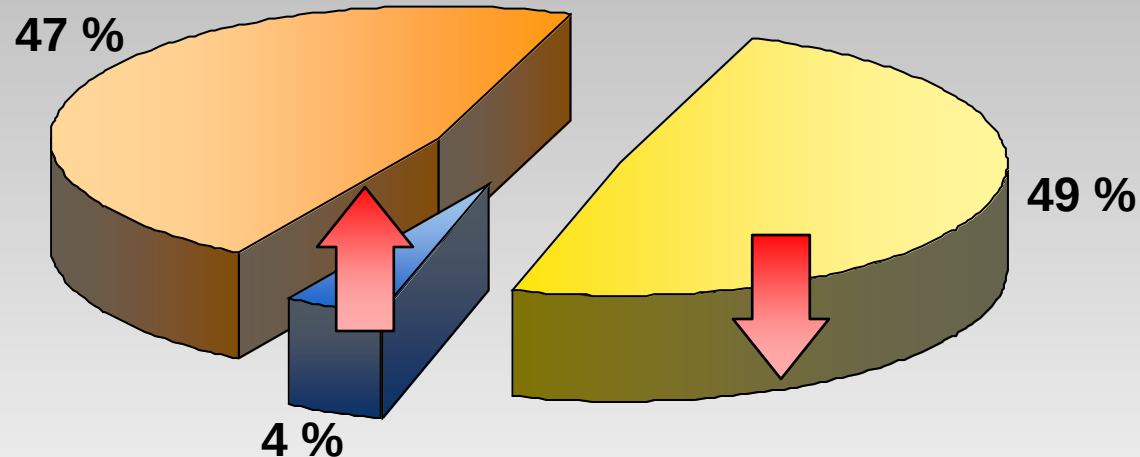
Turva-automaation toteutukset

Käytännön tuloksia turvaratkaisuista



Lähde

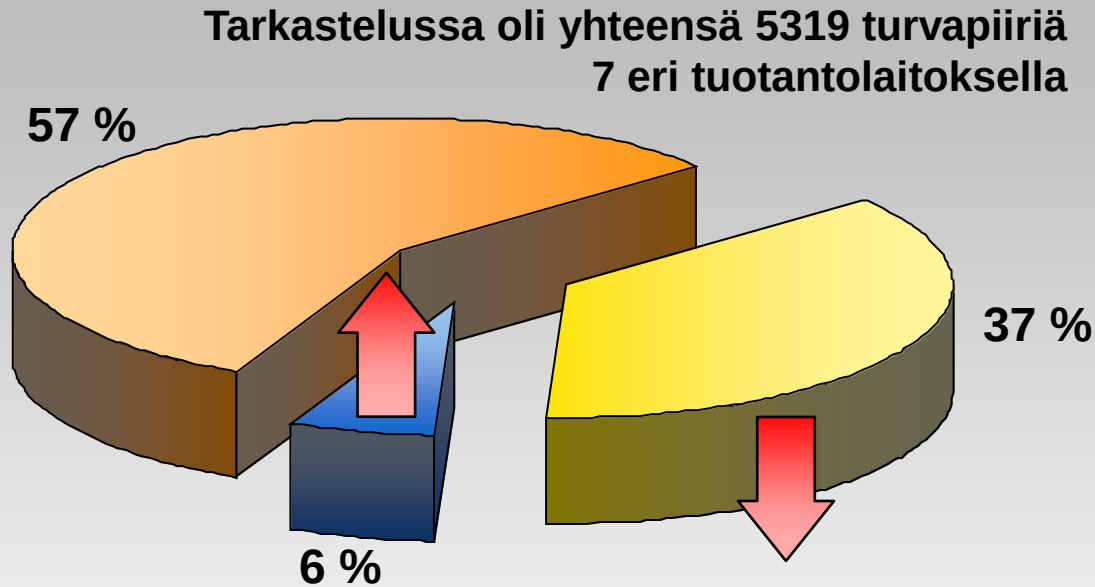
Öljynjalostamo: Vety-yksikkö



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

Turva-automaation toteutukset

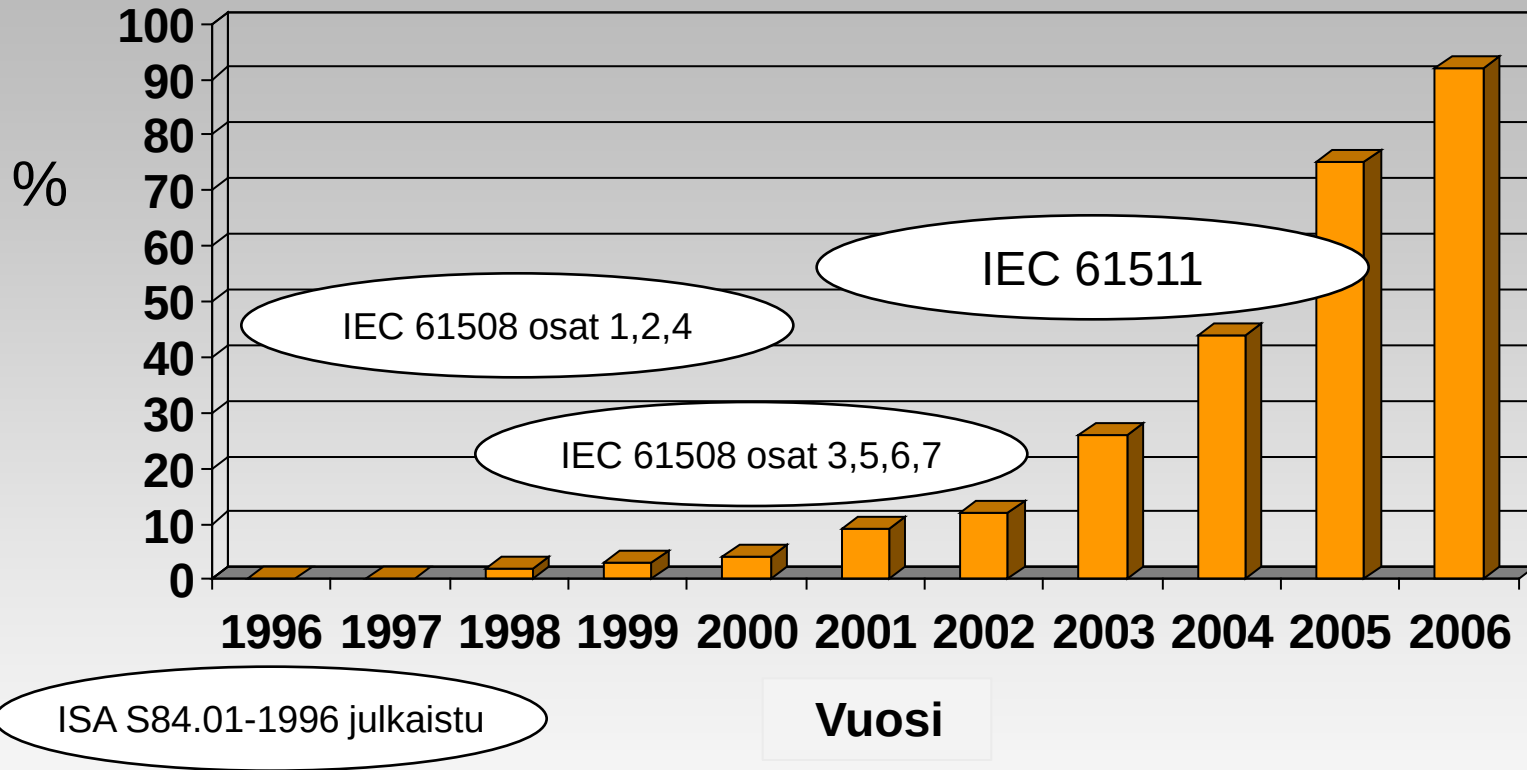
Käytännön tuloksia turvaratkaisuista



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?

Laitetaso - IEC 61508 sertifiointi



- 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

[PRODUCTS](#) | [SERVICES](#) | [TRAINING](#) | [TOOLS](#) | [COMPANY](#) | [MEMBER LOGIN](#) | [CONTACT](#) | [FORUM](#) | [STORE](#)

Home: [Tools](#) : Safety Automation Equipment List



Safety Automation Equipment List

Safety Equipment Selection

Careful selection of equipment used in automation safety is important. The quality, safety integrity and suitability for application must be understood.

To make this task easier, the Safety Automation Equipment List provides guidance on the tasks that need to be performed and a comprehensive list of products that have been third party evaluated per one of the recognized evaluation techniques as shown below.

Assessment Levels for Safety Equipment

1 STEP 1	Select potential product choices from the Safety Automation Equipment List.  Enter list	→ exSILentia™ Stand Alone → exSILentia™ On-Line → SILver™ → SILect & SRS → Member Login
2 STEP 2	Evaluate the product for suitability in your specific application.  Does the product meet all functional needs?  Are materials of construction compatible with the process chemistry?  Are environmental ratings sufficient for your environment?	
3 STEP 3	Evaluate the safety integrity of the product.  Does the product have a 61508 certification with a certification report?  IEC 61508 Certification Program FAQ  Open IEC 61508 Certification of Products  Does the certification report provide a description of the work performed that includes the design process and the analysis methods used. Step 3a: If no application suitable 61508 certified product is available, then prior use justification must be made per IEC 61511. A third party "Proven In Use" report or a third party FMEDA analysis will be valuable as part of the justification	

IEC 61508 sertifioituja turvalogii- koita



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	Prosafte-RS	Safety Controller / PLC	61508 Certified	TÜV Rh.			

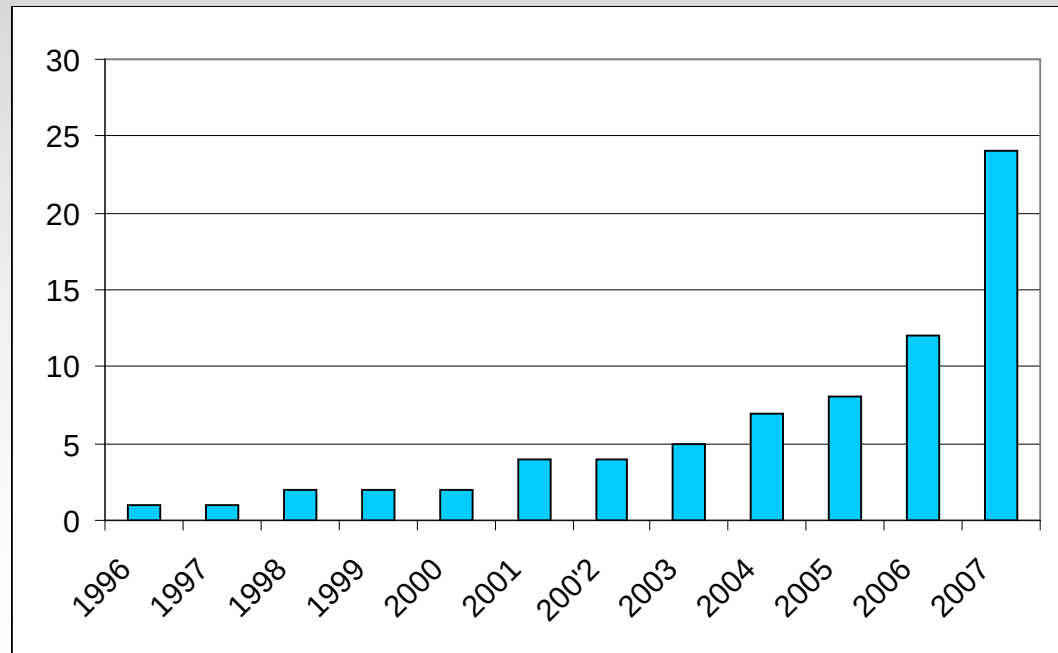
Company	Model	Description	Assessment	Assessor	Assessment Report	Contact	Link
Det-tronics	Eagle Quantum Premier	Fire and Gas Controller	61508 Certified	exida			
Det-tronics	ELS	Fire and Gas Controllers	61508 Certified	TÜV Rh.			
MSA	Suprema	Fire and Gas Controller	61508 Certified	TÜV Rh.			



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- lähettämiä



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			

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*/K VX*	Ball Segment Valve		FMEDA				
SOMAS Instrument	SKV	Ball Valve		FMEDA				



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 – tuotesertifiointin 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-tavoitetaso vaatimukset, systemaattiset viat on estetty riittävän hyvin
5. Turvaohje varmistamaan laitteen oikean käytön

Täysi tuote-
sertifiointi

Dokumentointi
käyttäjille - 5

Kehitysprosessin
sertifiointi – 3,4

Hardware – 1,2



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**