IEC61508 sovellusohjelmoinnissa

Suvi-Maaret Hyyryläinen
Yksikön päällikkö

MIPRO *Vahvaa osaamista*

suomeksi in English

Turvallisuuden ja ympäristötekniikan luotettava osaaja ja yhteistyökumppani

Kehitämme ja toimitamme kokonaisvaltaisia järjestelmäratkaisuja rautatieliikenteen ja teollisuuden turvallisuuden hallintaan sekä vesi- ja energiahuollon prosessien ohjaukseen ja valvontaan. Lue lisää

YRITYS | TOIMIALAT | REFERENSSIT | AJANKOHTAISTA | REKRYTOINTI | MEDIA | YHTEYSTIEDOT

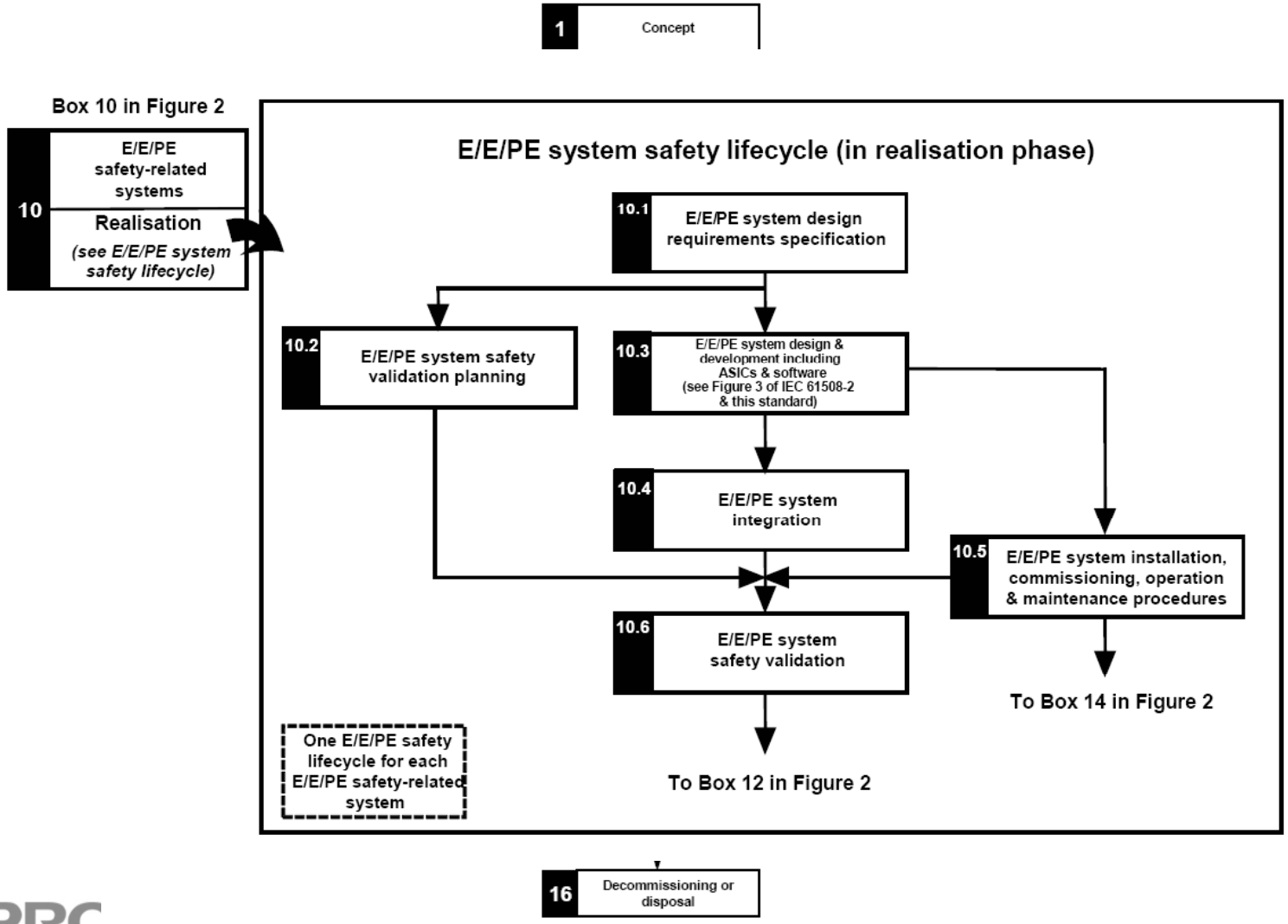
Rautatiejärjestelmät

Vesi- ja energiahuollon järjestelmät

Teollisuuden turvallisuuteen liittyvät järjestelmät

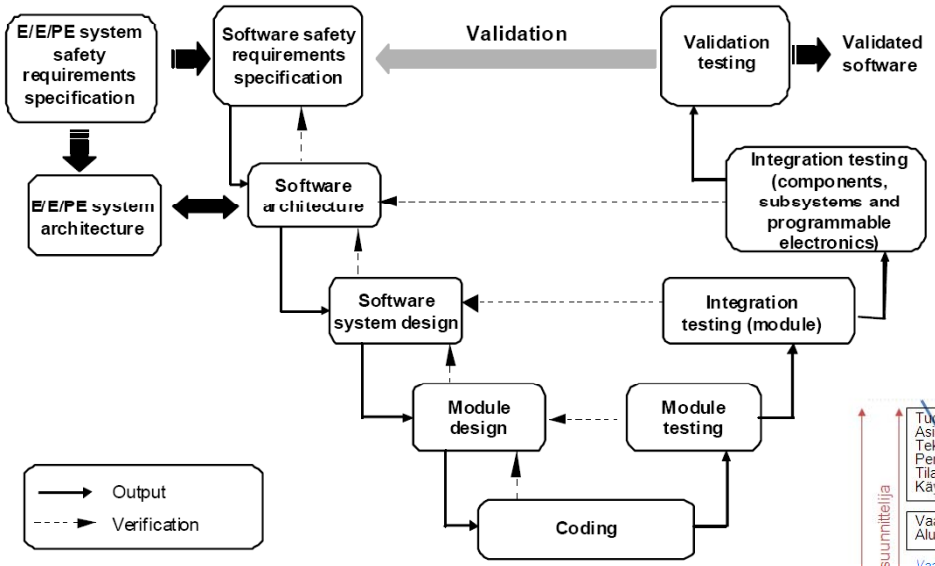
Konserni

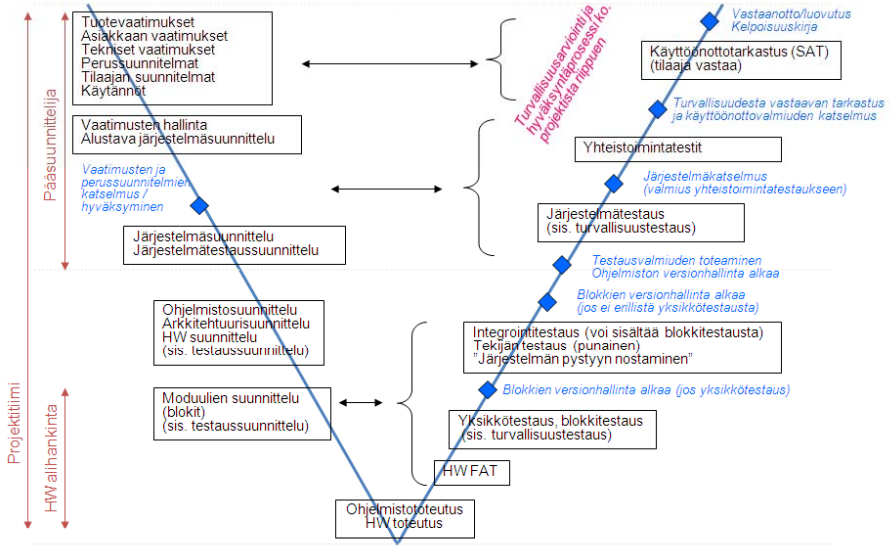
IEC61508 elinkaari – Mipro Scope



MIPRC

IEC 61508 V –malli vs. Mipro V -malli





Vaatimukset

- Vaatimukset asiakkaalta (tekniset, järjestelmän vaatimukset)
  - Ohjelmiston toiminnalliset vaatimukset
  - Ohjelmiston laadulliset vaatimukset
- Ympäristöön liittyvät vaatimukset

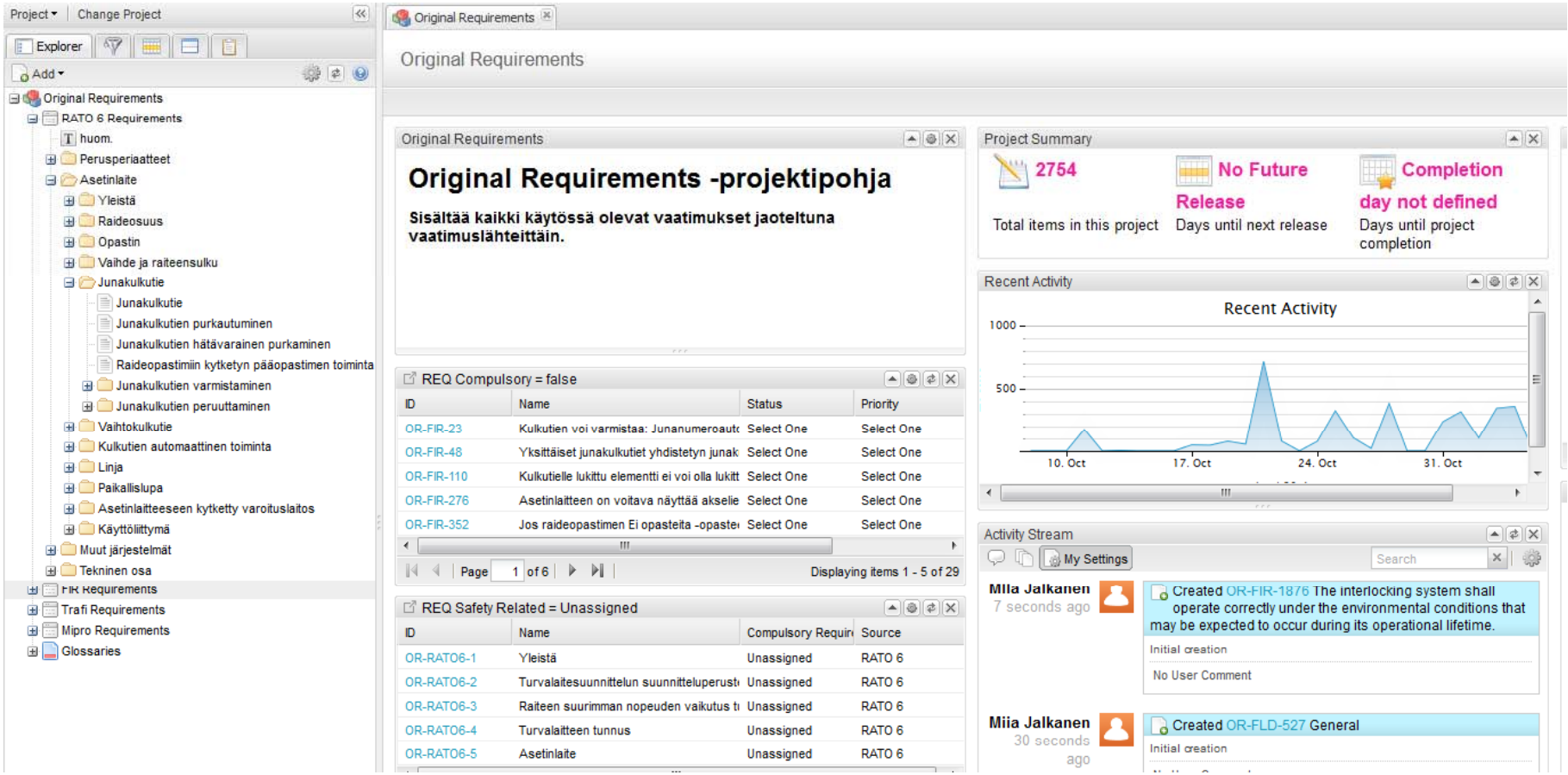
- Vaatimukset standardeista (menetelmät, tekniikat)
  - SIL taso?
  - Mikä standardi?
  - Mitkä osa-alueet?

Vaatimukset ⇨ Tuotokset

- ⇒ Projektinhallinta
  - ⇒ Safety plan
  - ⇒ Laatusuunnitelma
  - ⇒ Elinkaaren suunnitelma
  - ⇒ Verifiointisuunnitelma
  - ⇒ Validointisuunnitelma
- ⇒ Hazard Log (rautatieprojekteissa)
- ⇒ Vaatimusmäärittely
- ⇒ Järjestelmän laajuus

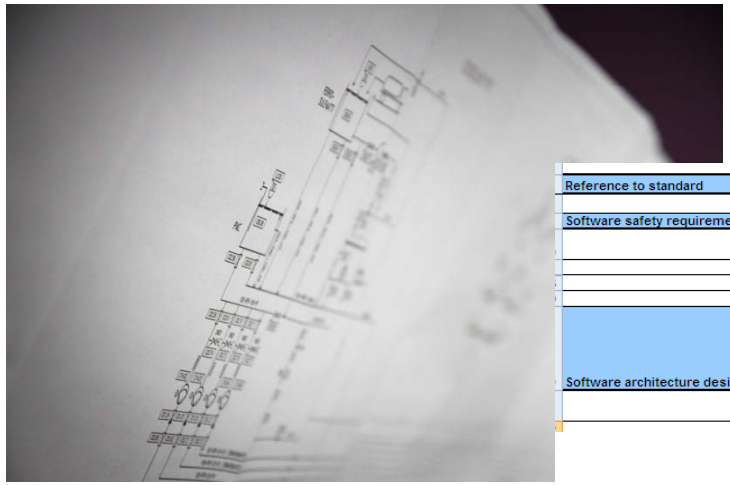
- ⇒ Verifiointiraportti
- ⇒ Hyväksyntä

Vaatimustenhallinta



Ohjelmistosuunnittelu -arkkitehtuuri

- Tärkeää pätevä, kokenut henkilö
- Vaatimusten kohdistaminen moduuleille
  - Hyväksytyt moduulit
- Muutosten suunnittelu
- Projektikohtainen toteutus
- Toteutustekniikat SIL – tason mukaan



Reference to standard	Technique		Justification	Reference to document
Software safety requirements specification (A1)				
1	Comp	Fault detection and diagnosis	The use of certified ELOP tool, Software architecture description	Software architecture Description
2a	Semi-	Error detecting and correcting codes		Software architecture Description
2b	Forma	Failure assertiong programming	N/A Limited variability programming	
		Safety bag techniques		
		Diverse programming		
		Recovery block		
		Backward recovery		
Software architecture design (A2)		Forward recovery		
		Re-try fault recovery mechanisms		
1	Fault	Memorising executed cases	Features of Hima system; Watchdog, timers, redundancy, I/O monitor, data range checking)	Software architecture Description
2	Error	Graceful degradation		
		Structured methods		
		Semi-formal methdos (B7)		
		Formal methods		
		Computer-aided specification tools		

Ohjelmistosuunnittelu ⇨ Tuotokset

⇒ Arkkitehtuurikuvaus

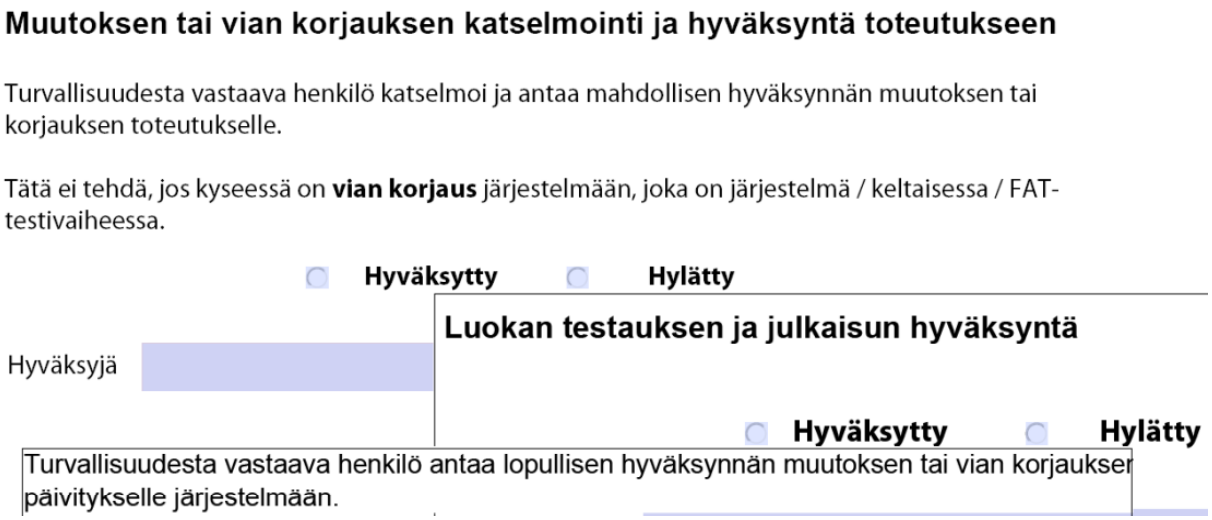
⇒ Järjestelmätestaus-suunnitelma

⇒ Verifiointiraportti

⇒ Hyväksyntä

⇒ Muutostenhallinta

⇒ Muutosten hyväksyntä



Muutoksen tai vian korjauksen katselmointi ja hyväksyntä toteutukseen

Turvallisuudesta vastaava henkilö katselmoi ja antaa mahdollisen hyväksynnän muutoksen tai korjauksen toteutukselle.

Tätä ei tehdä, jos kyseessä on **vian korjaus** järjestelmään, joka on järjestelmä / keltaisessa / FAT-testivaiheessa.

Hyväksytty Hylätty

Luokan testauksen ja julkaisun hyväksyntä

Hyväksyjä

Hyväksytty Hylätty

Turvallisuudesta vastaava henkilö antaa lopullisen hyväksynnän muutoksen tai vian korjauksen päivitykselle järjestelmään.

Ohjelmiston toteutus

- Ohjelmistomoduulit
- Ohjelmointi
- Moduulien testaus
- Henkilöiden pätevyys
  - Testaus
  - Muutokset
  - Versionhallinta
- Muutosten hyväksyntä
  - Moduulikirjasto
  - Hyväksytyt moduulit

- Katselmukset
- Pariohjelmointi (tutorointi)

Tuotokset

⇒ Lähdekoodi

⇒ Testauspöytäkirjat, -raportit

⇒ Versionhallinta

⇒ Verifiointiraportti

Ohjelmiston testaus

Integrointitestaus

- Ohjelmistomoduulien ja laitteiston integrointi
- Tekijän tekemä

Tuotokset

⇒ Ohjelmiston versionhallinta

⇒ Valmius järjestelmätestiin

Ohjelmiston testaus

Järjestelmätestaus

- Osa verifiointia (arkkitehtuuri, moduulit)
- Osa validointia (kriittiset vaatimukset)
- Simulointiympäristö (ohjelmisto, laitteet)
- Pätevät ja riippumattomat henkilö(t)
- Riippumattomuus suunnittelusta ja toteutuksesta

Tuotokset

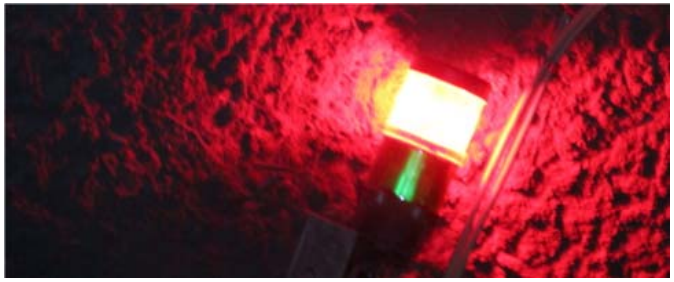
⇒ Testauspöytäkirjat, -raportti

On-Site testaus

- Osa validointia
- Kokonaisjärjestelmä
- Pätevät ja riippumattomat henkilöt
- Riippumattomuus suunnittelusta ja toteutuksesta

Tuotokset

=> Testauspöytäkirjat, -raportit



Jatkuvat toiminnot

- Vaatimusten hallinta
- Muutosten hallinta
- Verifiointi ja validointi

=> Päivitykset arkkitehtuuriin, moduuleihin, testaussuunnitelmiin ja testauksiin

Ohjelmiston hyväksyntä

- Hyväksytään ohjelmisto
- Pätevä henkilö (validoija)
- Riippumattomuus projektista
- Koko elinkaaren ajan

⇒ Valmius asiakkaalle toimitettavaksi

⇒ Ei puutteita (turvallisuus, käytettävyys, suorituskyky)

⇒ Järjestelmätestaus, on-site testaus

⇒ Versionhallinta, konfiguraationhallinta

⇒ Dokumentaatio ajantasalla (koko elinkaari)

⇒ Henkilöiden pätevyys ja riippumattomuus

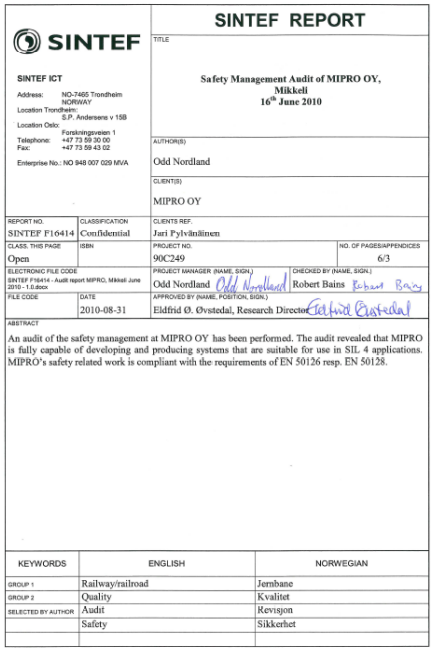
⇒ Standardin vaatiman tason mukainen

SILx –tason järjestelmän toteutus

- Hyväksytyt laitteet
- Hyväksytyt työkalut
- Hyväksytyt ohjelmistomoduulit

- Hyväksytyt menetelmät
- Hyväksytyt suunnittelutekniikat

- Osaava henkilöstö



SINTEF

SINTEF ICT

Address: NO-7465 Trondheim NORWAY
Location Trondheim: S.P. Andersens v 15B
Location Oslo: Forskningsveien 1
Telephone: +47 73 59 30 00
Fax: +47 73 59 43 02
Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

Safety Management Audit of MIPRO OY, Mikkeli 16th June 2010

AUTHOR(S)

Odd Nordland

CLIENT(S)

MIPRO OY

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
SINTEF F16414	Confidential	Jari Pylvänäinen	
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Open		90C249	6/3
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
SINTEF F16414 - Audit report MIPRO, Mikkeli June 2010 - 1.0.docx		Odd Nordland	Robert Bains
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2010-08-31	Eldfrid Ø. Øvstedal, Research Director	

ABSTRACT

An audit of the safety management at MIPRO OY has been performed. The audit revealed that MIPRO is fully capable of developing and producing systems that are suitable for use in SIL 4 applications. MIPRO's safety related work is compliant with the requirements of EN 50126 resp. EN 50128.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Railway/railroad	Jernbane
GROUP 2	Quality	Kvalitet
SELECTED BY AUTHOR	Audit	Revisjon
	Safety	Sikkerhet

inland®

malainen

ng Professionals

and has met the approval criteria for a

TÜV Functional Safety Engineer
Safety Instrumented Systems

Certificate Number: TÜVFSEng 724/07
Issue date: June 200?
Expiry date: June 2012

Cologne, June 2007

TÜV Rheinland Industrie Service GmbH
Automation, Software
and Information Technology (ASI)

Dipl.-Ing. Heinz Gall
Head of TÜV Functional Safety Program

Functional Safety Engineer
Safety Instrumented Systems
ID: 724/07

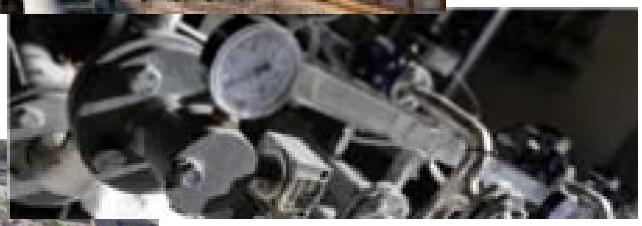
TÜVRheinland® FSEngineer

Kehityksen alla

- Paljon dokumentaatio => Dokumentaation ajantasaisuus
- Vaatimusten hallinta
- Testauksen jaksottaminen
- Muutosten vaikutukset
- Kommunikointi

- Henkilöstön osaaminen => vaatimuksia koulutus, työkokemus, työtehtävät
- Tiimityö => kaikki tekevät työtä saman asian eteen
- Arvot => Vaatimukset, testaus

Kiitos!



www.mipro.fi