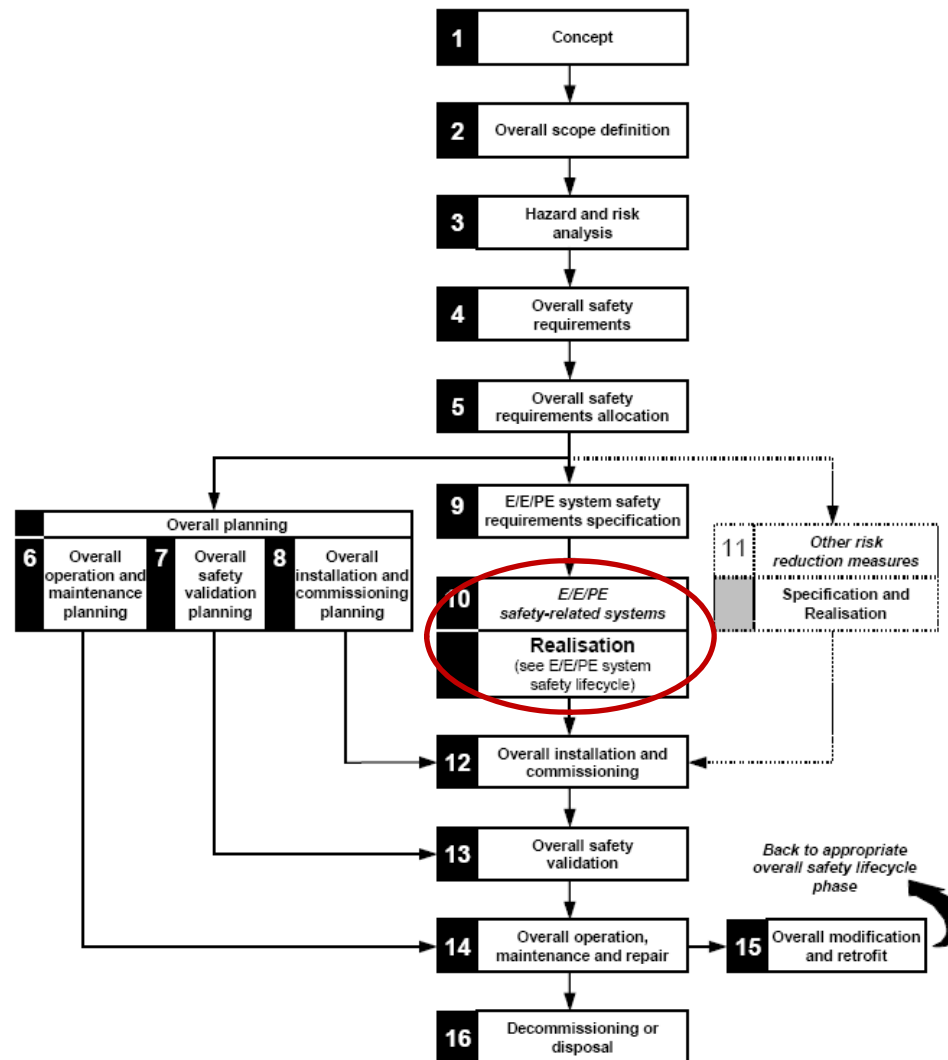


# IEC61508 – osa 3 ohjelmistovaatimusten soveltaminen

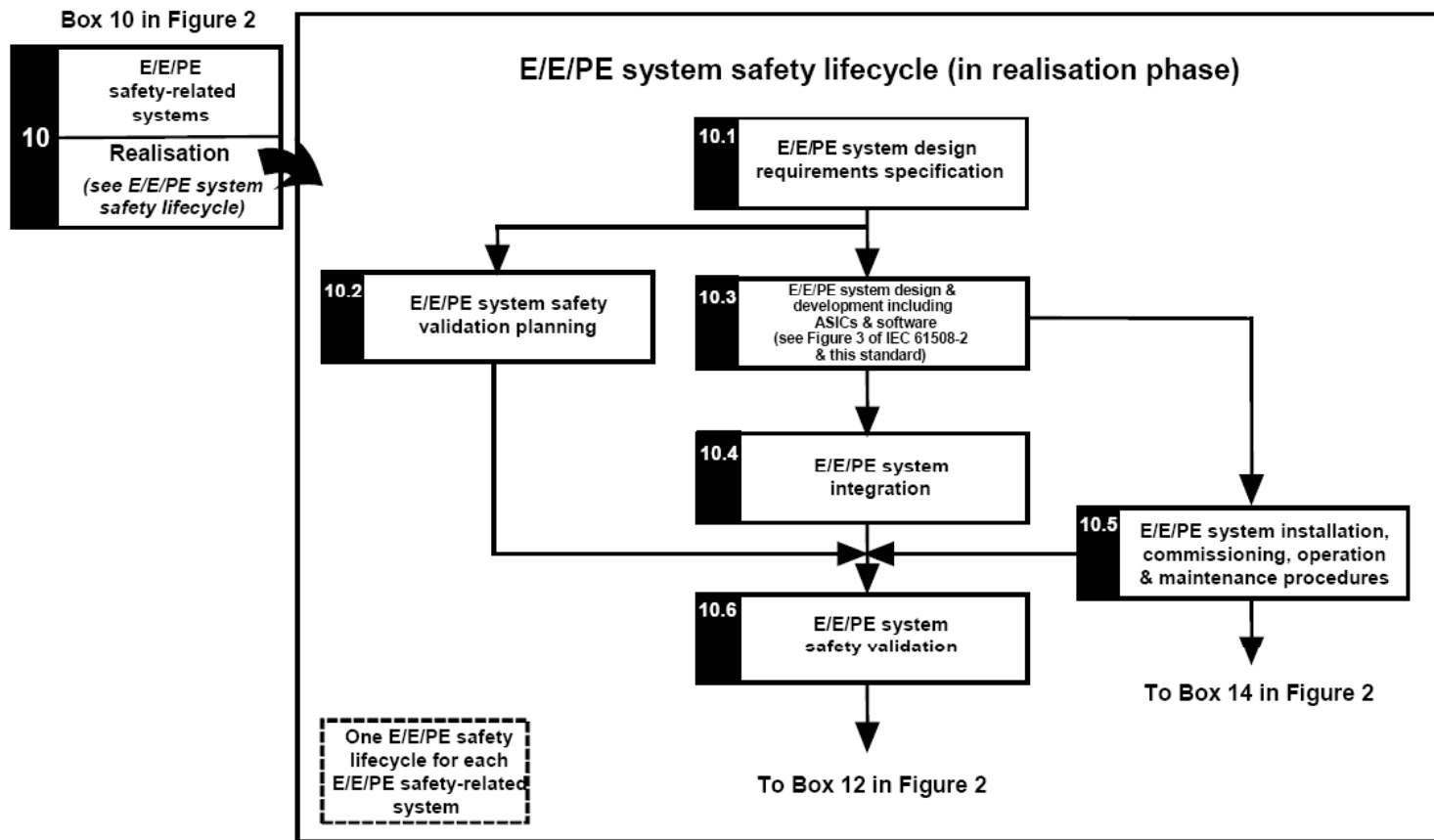
Suvi-Maaret Hyyryläinen  
Yksikön päällikkö, Mipro Oy

**MIPRO**

# IEC61508 elinkaari – Mipro Scope



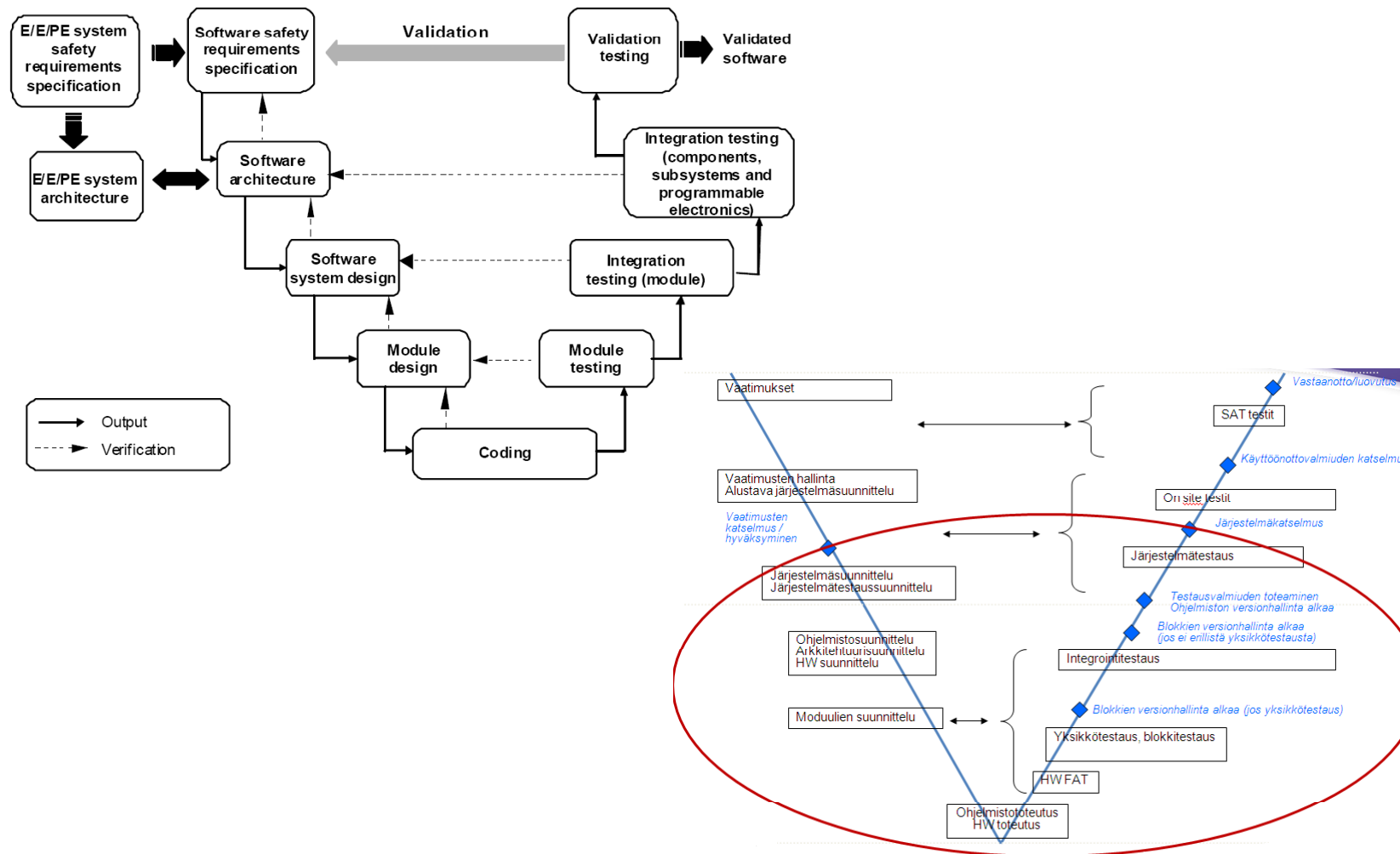
# IEC61508 elinkaari – Mipro Scope



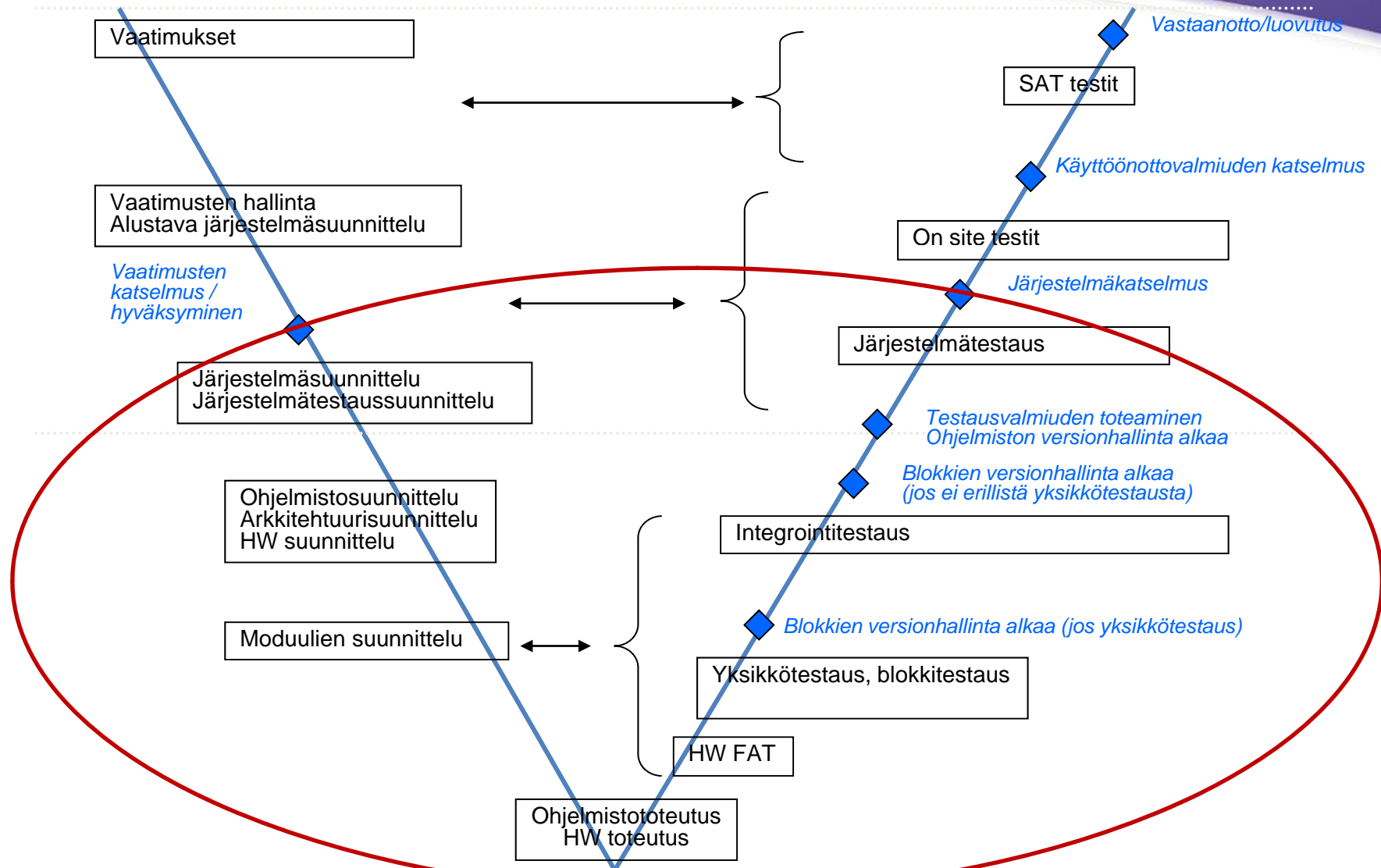
# SILx –tason järjestelmän toteutus

- Hyväksytyt laitteet
- Hyväksytyt työkalut
- Hyväksytyt ohjelmistomoduulit
  
- Hyväksytyt menetelmät
- Hyväksytyt suunnittelutekniikat
  
- Osaava henkilöstö
  - TÜV FS Engineer/Professional
  - Työkokemus
  - Muu koulutus

# IEC 61508 V –malli vs. Mipro V -malli



# Järjestelmätoteutus (V-malli) Mipro



# Vaatimukset

- Vaatimukset asiakkaalta (tekniset, järjestelmän vaatimukset)
    - ⇒ elinkaaren suunnitelma
    - ⇒ verifiointisuunnitelma
    - ⇒ validointisuunnitelma
    - Järjestelmän toiminnalliset vaatimukset ⇒ Hazard Log
    - ⇒ Vaatimusmäärittely
  - Vaatimukset standardeista (menetelmät, tekniikat) ⇒ Verifiointi
    - SIL taso?
    - Mikä standardi?
    - Mitkä osa-alueet?
- ⇒ Projektinhallinta
- ⇒ safety plan
  - ⇒ laatusuunnitelma

# Ohjelmistosuunnittelu -arkkitehtuuri

- Vaatimusten kohdistaminen moduuleille ⇒ Arkkitehtuurikuvaus
- Hyväksytyt moduulit ⇒ Järjestelmätestaus-suunnitelma
- Muutosten suunnittelu ⇒ Verifiointi
- Projektikohtainen toteutus ⇒ Muutostenhallinta
- Toteutustekniikat SIL – tason mukaan ⇒ Muutosten hyväksyntä



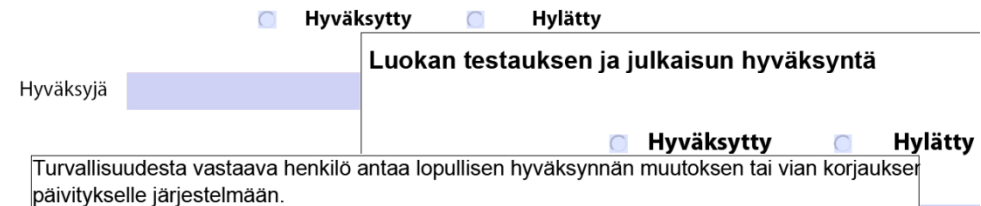
# Ohjelmiston toteutus

- Ohjelmistomoduoilit
- Ohjelmointi
- Moduulien testaus
- Henkilöiden pätevyys
  - Testaus
  - Muutokset
  - Versionhallinta
- Muutosten hyväksyntä
- Katselmukset

## 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.



- ⇒ Lähdekoodi
- ⇒ Testauspöytäkirjat, -raportit
- ⇒ Versionhallinta
- ⇒ Verifiointi

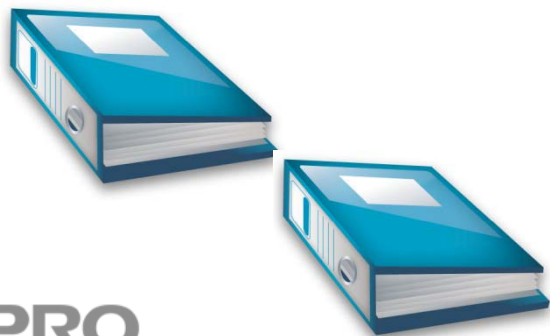
# Ohjelmiston testaus

## Integrointitestausta

- Ohjelmistomodulien ja laitteiston integrointi
- Tekijän tekemä

⇒ Ohjelmiston versionhallinta

⇒ Valmius järjestelmätestiin



## Järjestelmätestaus

- Validointi
- Simulointiympäristö (ohjelmisto, laitteet)
- Pätevä henkilö
- Riippumattomuus suunnittelusta ja toteutuksesta

⇒ Testauspöytäkirjat, -raportti

# Ohjelmiston hyväksyntä

- Hyväksytään ohjelmisto
  - Pätevä henkilö
  - Riippumattomuus projektista
- 
- ⇒ Valmius asiakkaalle toimitettavaksi
  - ⇒ Ei turvallisuuspuutteita
  - ⇒ Ei testauspuutteita
  - ⇒ Dokumentaatio ajantasalla
  - ⇒ Henkilöiden pätevyys ja riippumattomuus
  - ⇒ Standardin vaatiman tason mukainen



# IEC61508 osa 3 – uusi versio

- Helpommin sovellettavissa (annex C)
- Sopii paremmin järjestelmätoimittajillekin
- Tekniikat
  - Mallipohjainen testaus
  - Ketterät menetelmät
  - Tutkiva testaus



**Kysymyksiä?**

**Kiitos!**