# STUK:n vaatimukset automaation suunnittelulle ja toteutukselle

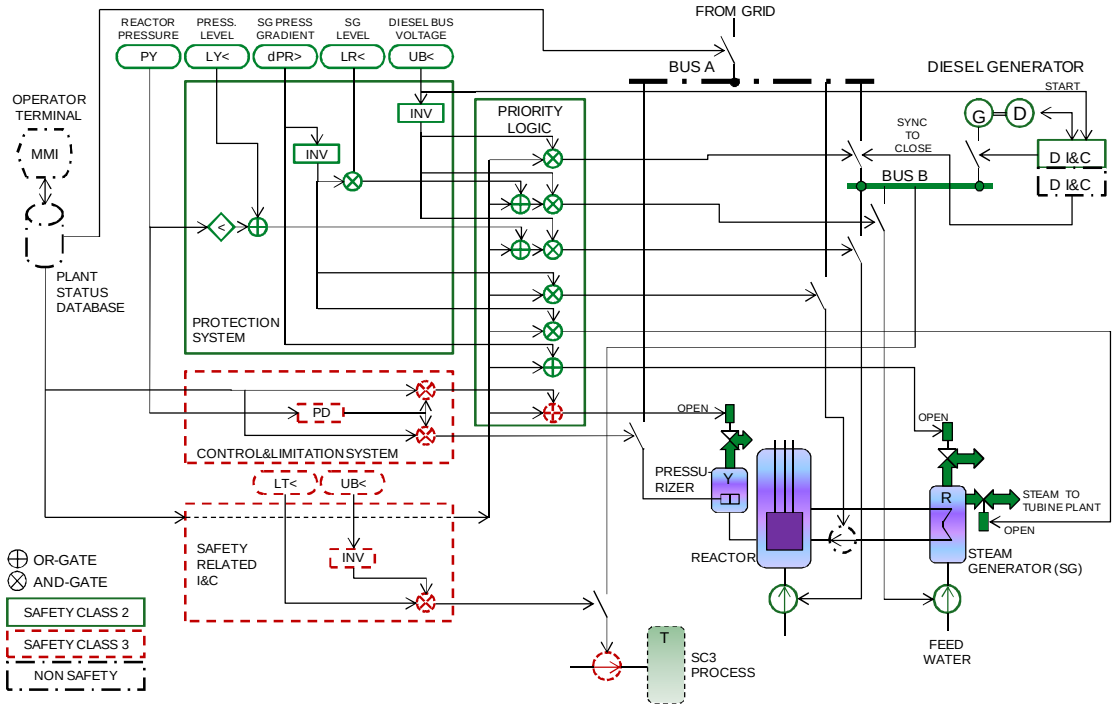
## ATS Syysseminaari 21.11.2014

# Automaatiojärjestelmien on oltava yhteensopivia ydinlaitoksen kokonaisturvallisuustavoitteiden kanssa

Järjestelmien on oltava yhteensopivia valvottavien / suojattavien / ohjattavien voimalaitosprosessien ja puolustuslinjojen kanssa

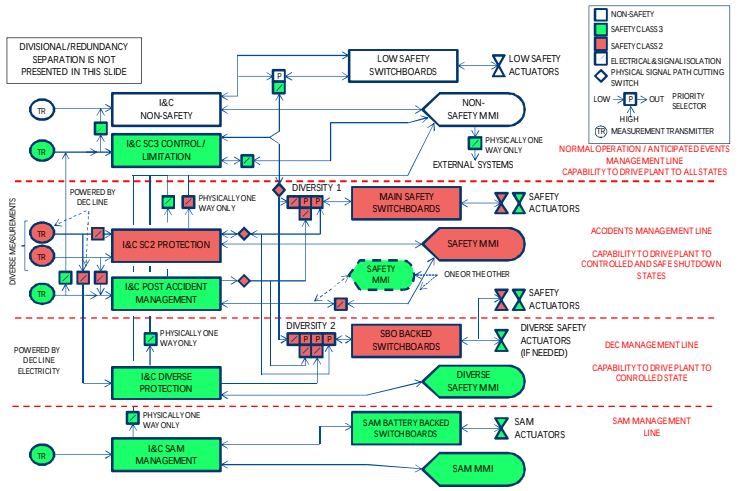
Erityisesti on huomioitava:

- Syvyyspuolustuksen toteutuminen ja puolustuslinjojen itsenäisyys (riippumattomuus) laitostasolla
- Vikakriteerivaatimusten toteutuminen (N+2 ja N+1) laitostasolla
- Erilaisuusperiaatteen toteutuminen laitostasolla
- Ympäristöolosuhteiden kesto



# Arkkitehtuuri, eli automaatiojärjestelmäkokonaisuuden yhteistoiminnan huomioiminen laitostasolla

- Arkkitehtuuritason suunnittelun merkitys on korostunut nykyaikaista ohjelmistopohjaista automaatiota käyttävillä laitoksilla
  - ”Wanhan ajan” automaatiossa järjestelmät olivat tekniikan rajoitusten vaikutuksesta luonnostaan melko itsenäisiä
  - Nykyisillä väyläpohjaista tiedonsiirtoa käyttävillä tekniikoilla on helppo luoda monimutkaisia riippuvuuksia eri toimintojen, järjestelmien ja puolustuslinjojen välille
  - Selkeät ”fysiikan lakeihin” perustuvat vikojen leviämistavat virtapiireissä ovat korvautuneet ”virtuaaliympäristöillä”, joissa vikojen leviämien on vaikeammin ennustettavaa ja hallittavaa




⇒ Toisiaan varmentavien perättäisten puolustuslinjojen riippumattomuus on varmistettava arkkitehtuuritasolla laadittavilla suunnittelusäännöillä ja arkkitehtuuritasolle tehtävällä testauksella ja analyyseillä

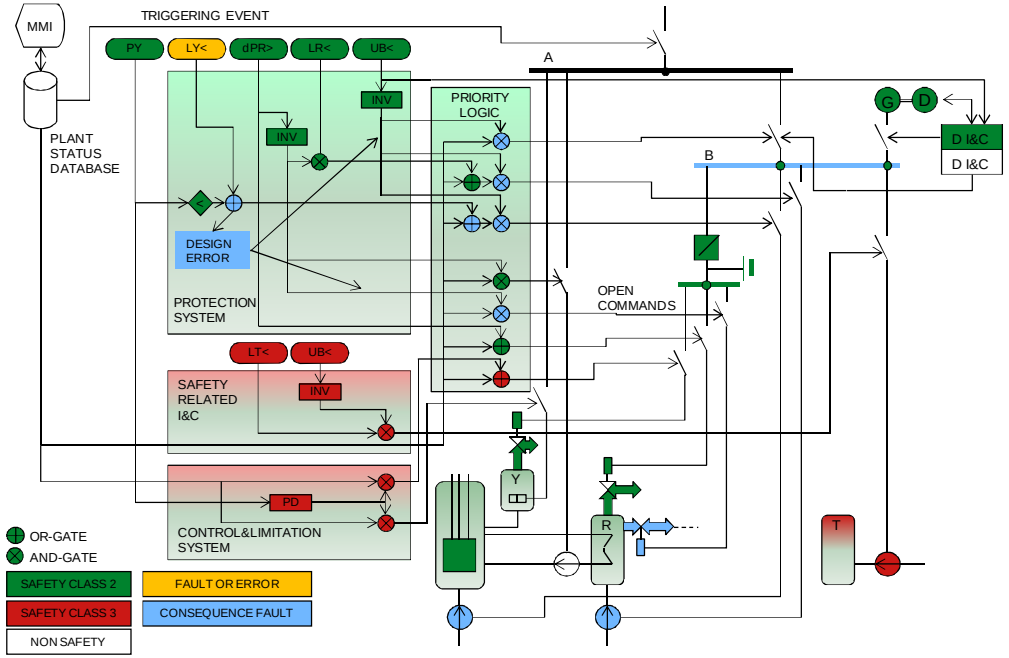
⇒ Seuraavan puolustuslinjan on kyettävä rajoittamaan edellisen linjan virhetoiminnan tai vian laitostason seuraukset hyväksyttäviksi

⇒ Arkkitehtuuritasolla täytyy luoda perusta myös järjestelmien tietoturvaratkaisuille

# Automaatiojärjestelmiltä vaadittavat ominaisuudet 1/2

Automaatiojärjestelmän on täytettävä yleiset ydinlaitoksen järjestelmävaatimukset

- Monikertaisuus, erilaisuus, erottelu sekä syvyyssuuntainen puolustus
  - Perustuvat toiminnallisuus-, luotettavuus- ja vikasietoisuusvaatimuksiin
- Luotettavuusvaatimukset
  - Turvallisuusluokitus on tehty luotettavuusvaatimusten perusteella, joten se vaikuttaa suoraan myös automaatiojärjestelmien laatuvaatimuksiin



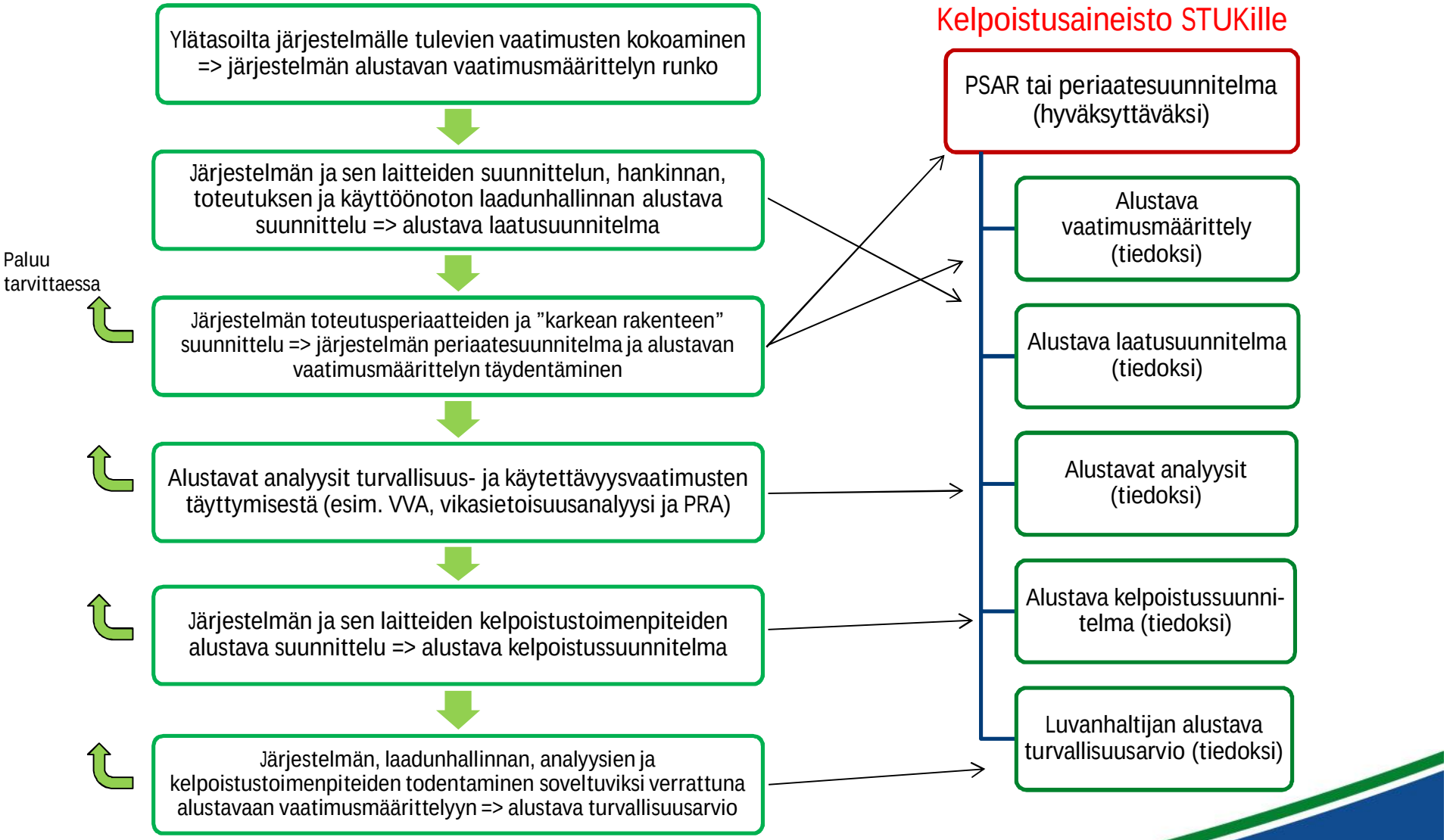
# Automaatiojärjestelmiltä vaadittavat ominaisuudet 2/2

- Yhteensopivuus laitosympäristön kanssa
  - Kelpoistaminen ympäristöolosuhteisiin, kuten onnettomuustilanteen aikaiset olosuhteet tai seisminen ja muu värähtelykestoisuus
  - Sähköiset häiriöt, sähkömagneettinen yhteensopivuus (EMC)
  - Tietoturvallisuus
  - Käyttöliittymä, langaton ohjaus

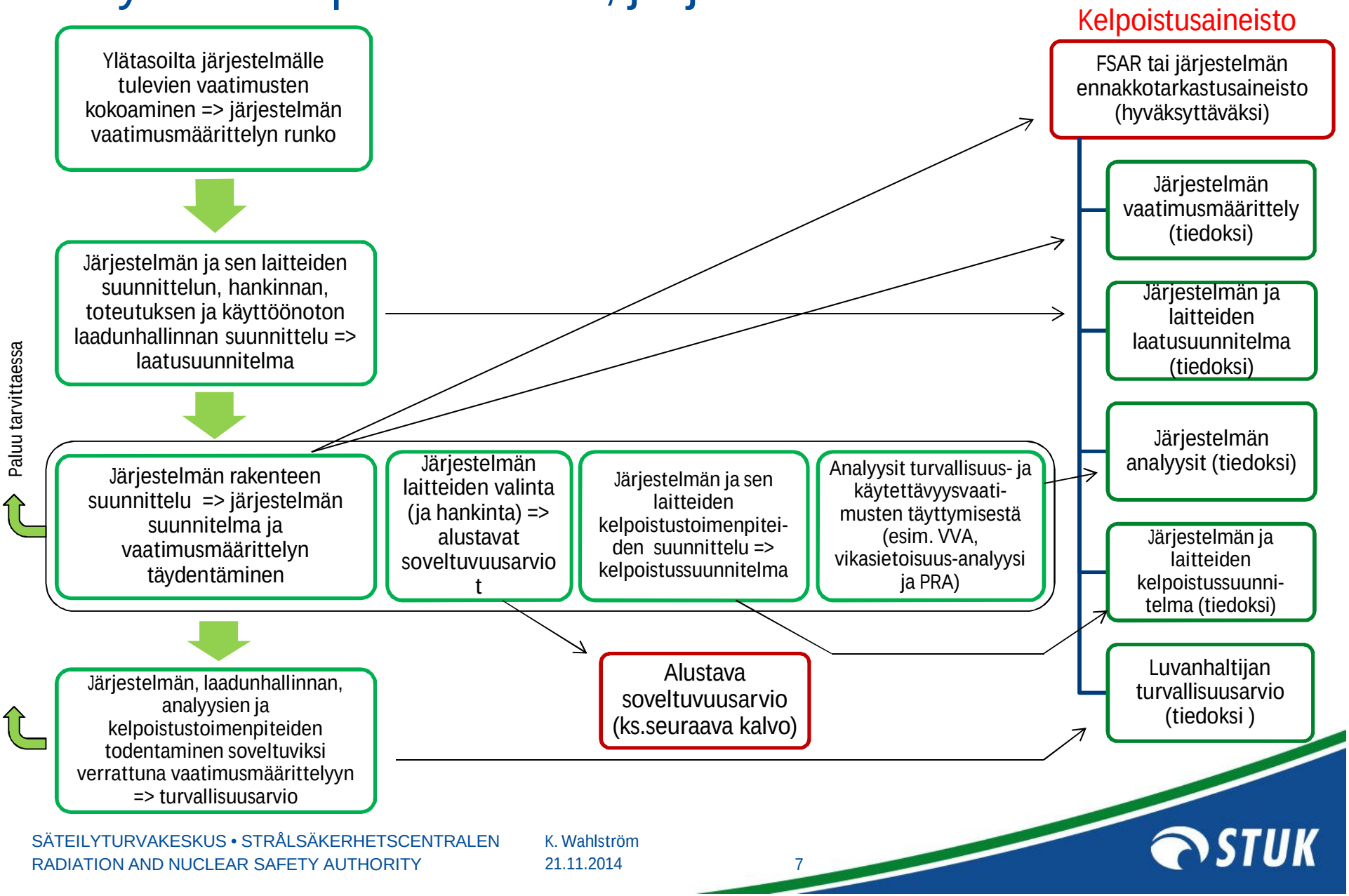
- Kelpoisuuden osoitus täydellisellä testauksella on usein ja varsinkin ohjelmistopohjaisessa tekniikassa mahdotonta, koska testattava tila-avaruus on liian laaja, mitä puutetta kompensoidaan:
  - Vaiheistamalla tarkkaan suunnittelu ja testaus (suunnittelun elinkaarimalli, V&V)
  - Dokumentoimalla (vaatimustenhallinta, konfiguraationhallinta)
  - Hallitsemalla jäännösriskiä seuraavalla puolustuslinjalla

- järjestelmien toiminta on kyettävä koestamaan määrävälein

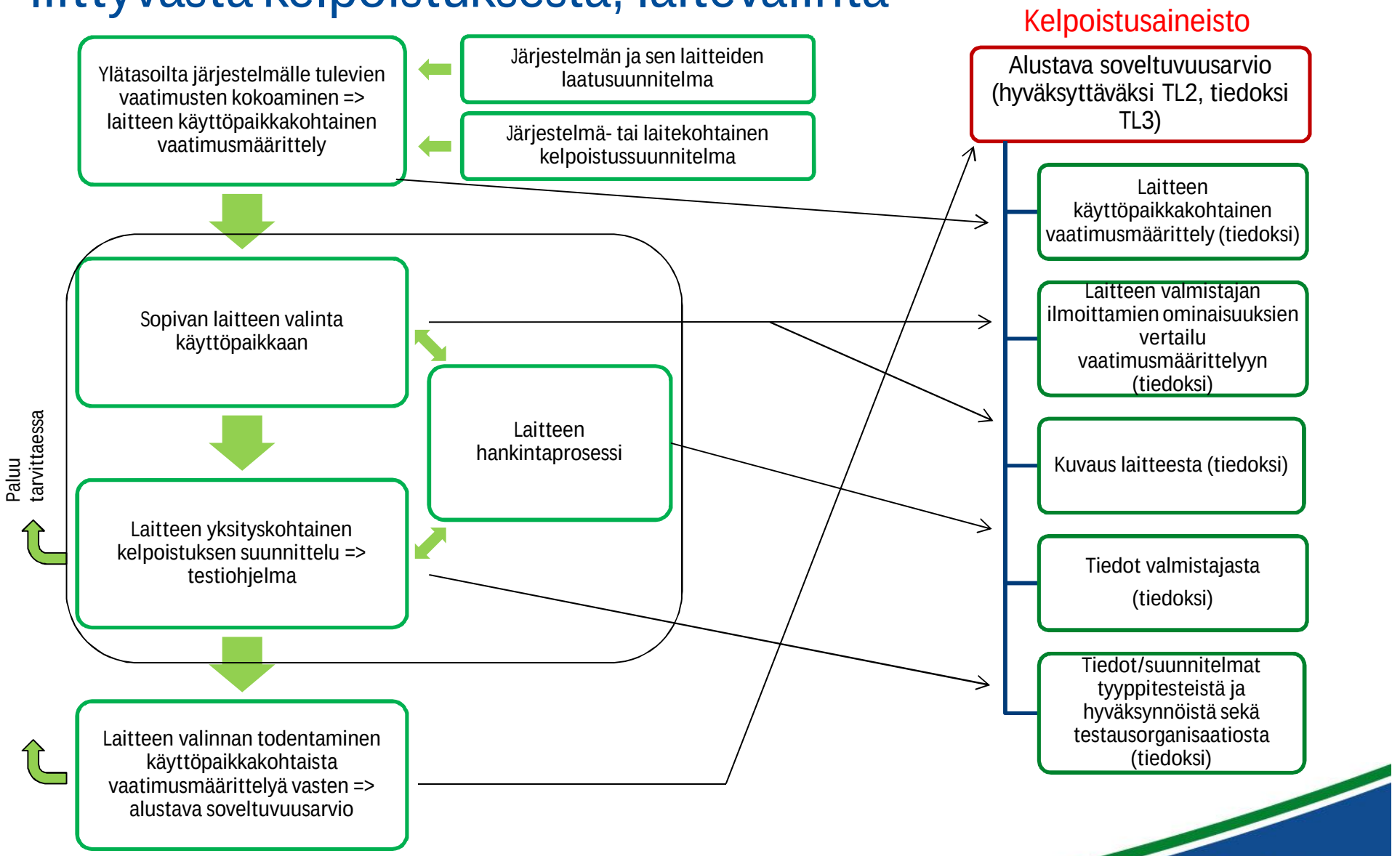
# Esimerkki automaatioprojektin vaiheistuksesta ja siihen liittyvästä kelpoistuksesta, periaatesuunnitteluvaihe



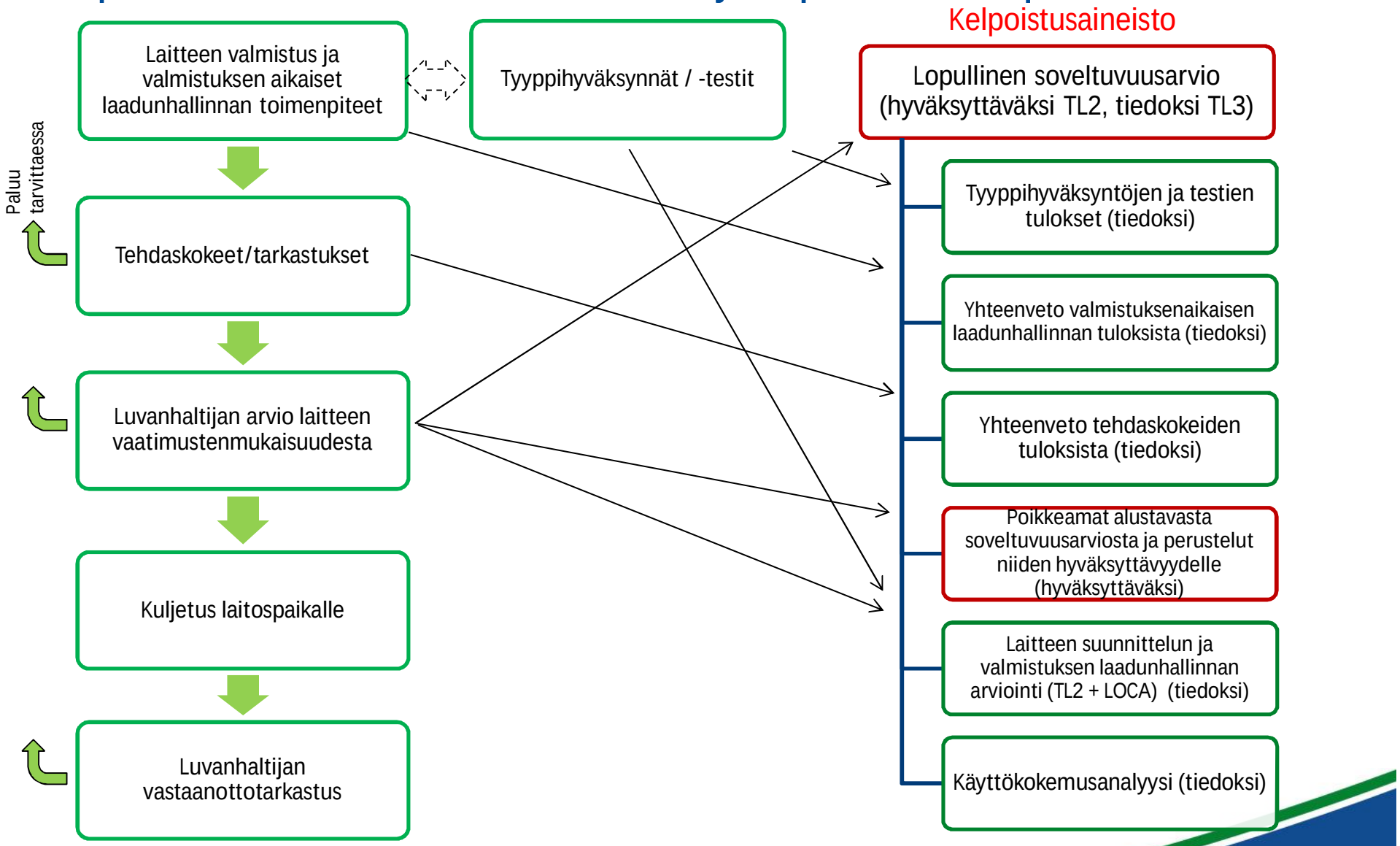
# Esimerkki automaatioprojektin vaiheistuksesta ja siihen liittyvästä kelpoistuksesta, järjestelmäsuunnitteluvaihe



# Esimerkki automaatioprojektin vaiheistuksesta ja siihen liittyvästä kelpoistuksesta, laitevalinta



# Esimerkki automaatioprojektin vaiheistuksesta ja siihen liittyvästä kelpoistuksesta, laitteen valmistus ja lopullinen kelpoistus



# Esimerkki automaatioprojektin vaiheistuksesta ja siihen liittyvästä kelpoistuksesta, asennus ja käyttöönotto