



Automaation elinkaari ja tietoturva

Automaation tietoturvallisuuden
teemapäivä

16.10.2013

Rosendahl/Tampere

Jari Seppälä?



- Automaation tietoturva-asiantuntija
- Opetus ja tutkimus
 - Sovellettu pehmoaskenta 1995-1999
 - Automaatio- ja informaatioverkot 1999-2013
 - Automaation tietotekniikka 2013 ⇒

"Luotettavaa automaatiota tietoturvan avulla"



Esityksen tavoite

Herättää
keskustelua sekä
ajatuksia ja
tietolähteitä
kotiinvietäväksi



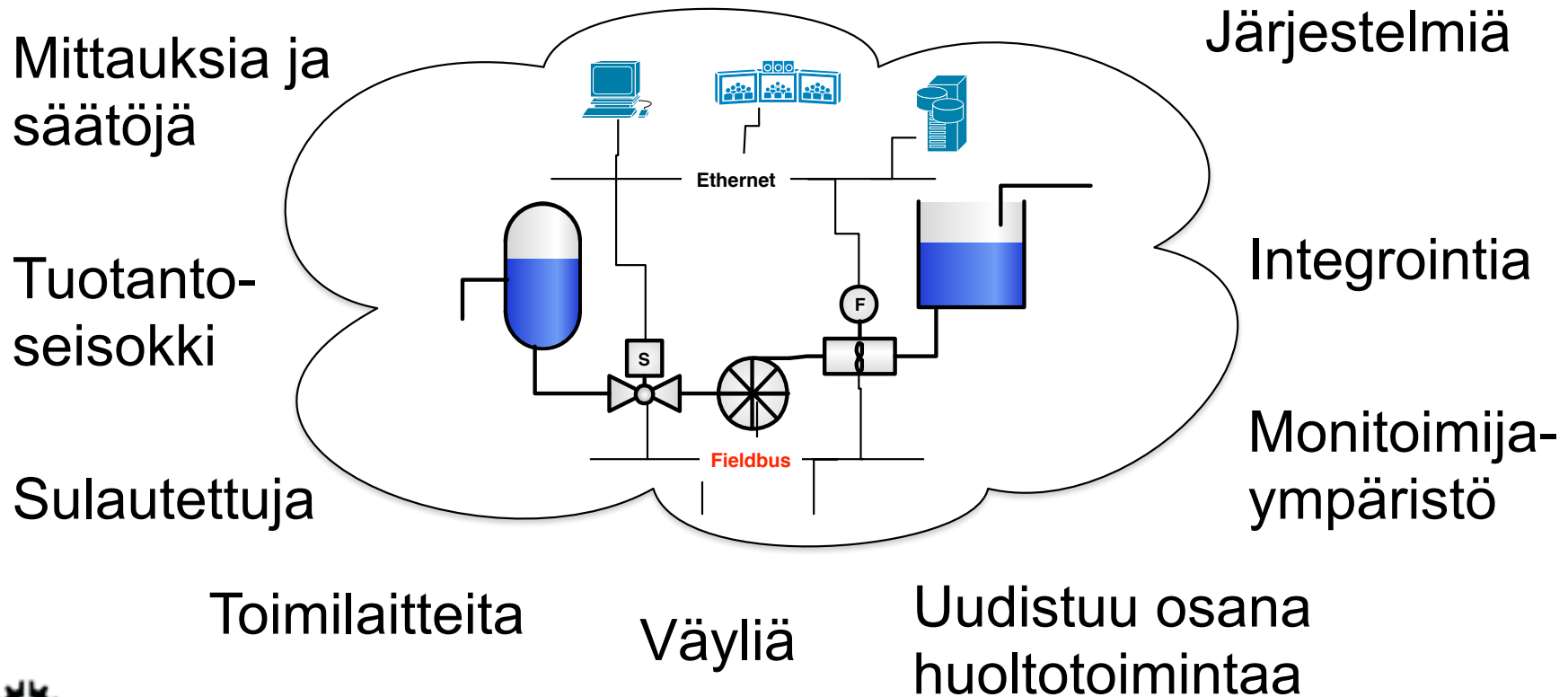
Agenda

- Automaatio?
- Automaation elinkaari
- Automaatio, reaaliaikaisuus ja miksi tietoturva on vaikeaa
- Tietoturva automaation elinkaareissa
- Suomen automaation tietoturvatyön elinkaari
- Kysymyksiä ja keskustelua

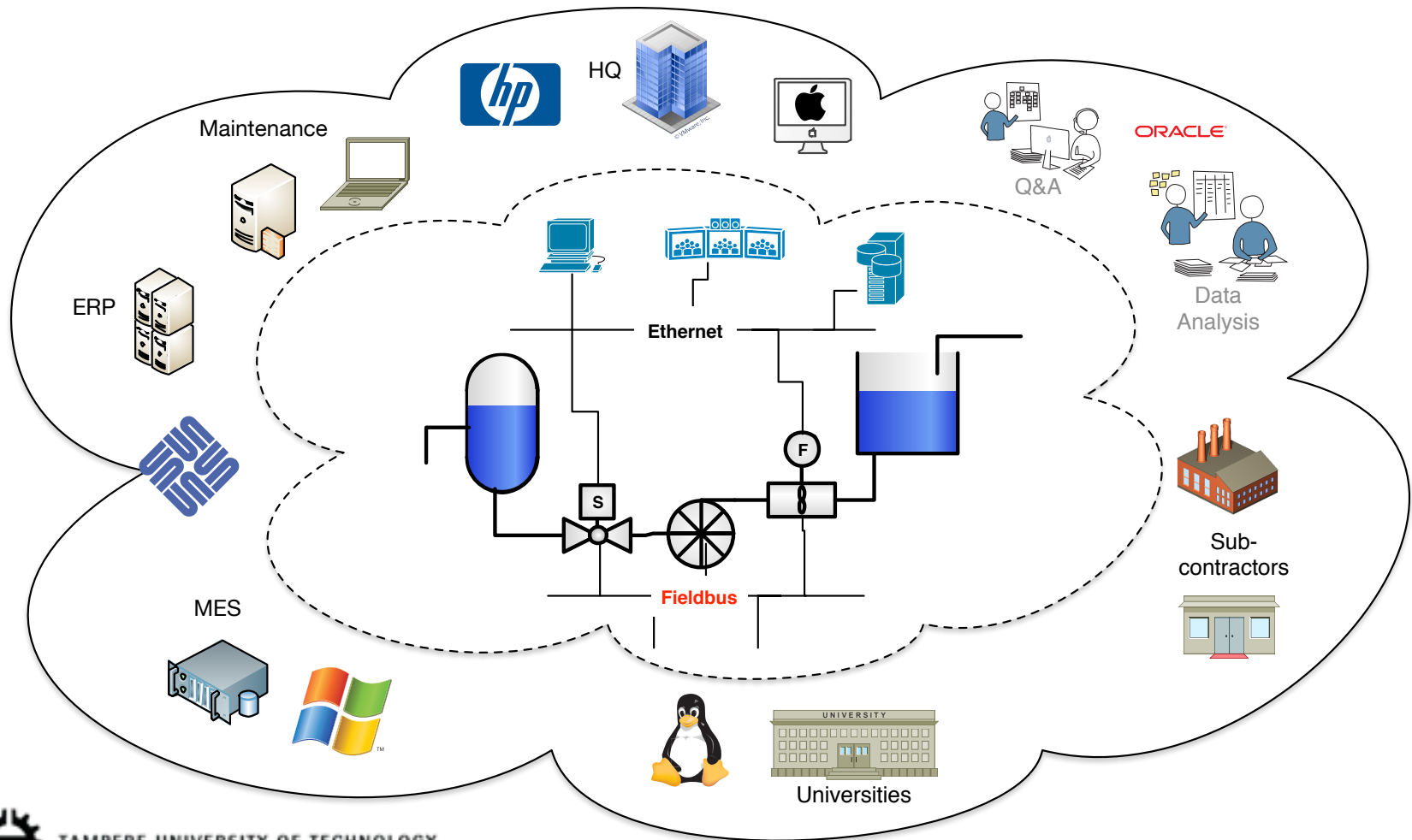


Automaatio – päivityssykli on $n \times 10v$, missä $n > 1$

Verkottunut ohjelmistotuote



Automaation reunalla tapahtuu – päivityssykli noin 3v



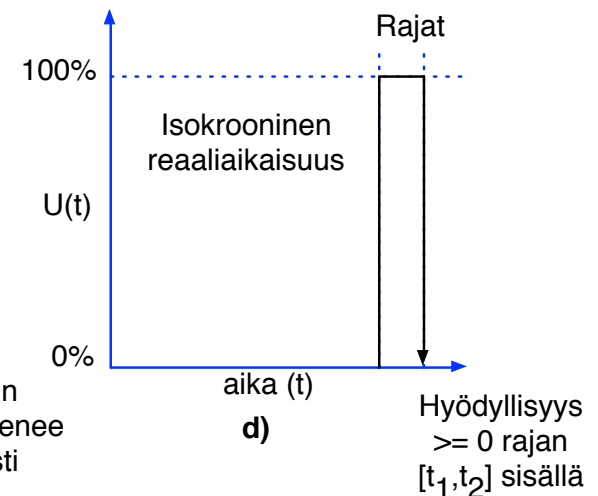
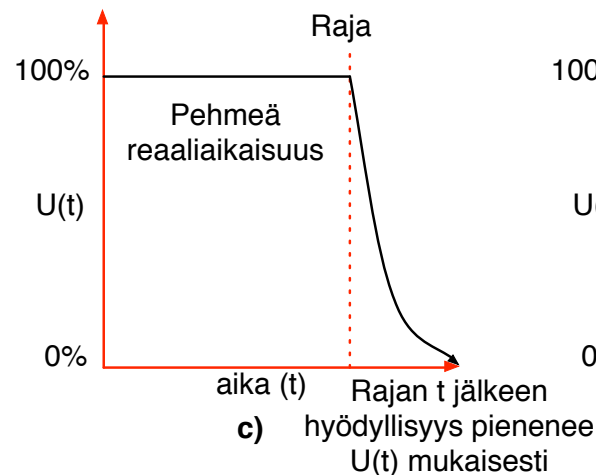
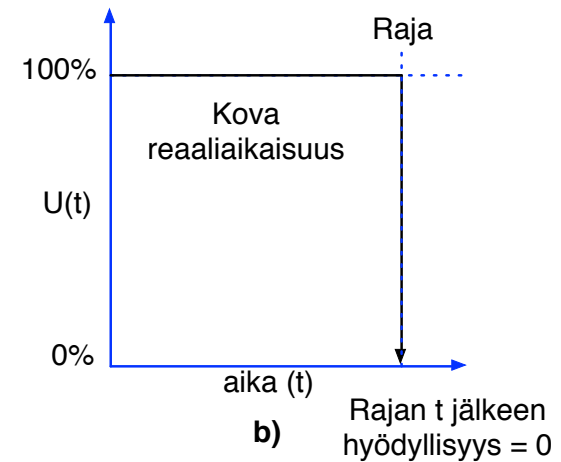
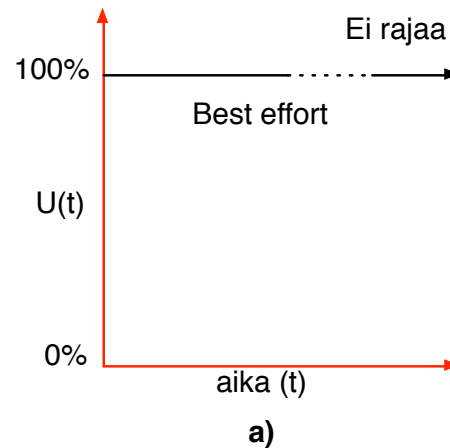
Automaation elinkaari

- Automaatiojärjestelmät elävät useita kymmeniä vuosia
- Automaation ”ytimen” uudistaminen on aina liiketoimintapäätös
 - Osaprosessi saattaa päivittyä esim. 5 vuoden välein
 - Aina harkittu ja suunniteltu toimenpide
- Reunalla tapahtuu jatkuvasti
 - Uudistaminen IT:n päivityssyklin mukaan



Automaatio, reaaliaikaisuus ja miksi tietoturva on vaikeaa

Tiedon
hyödyllisyys $U(t)$



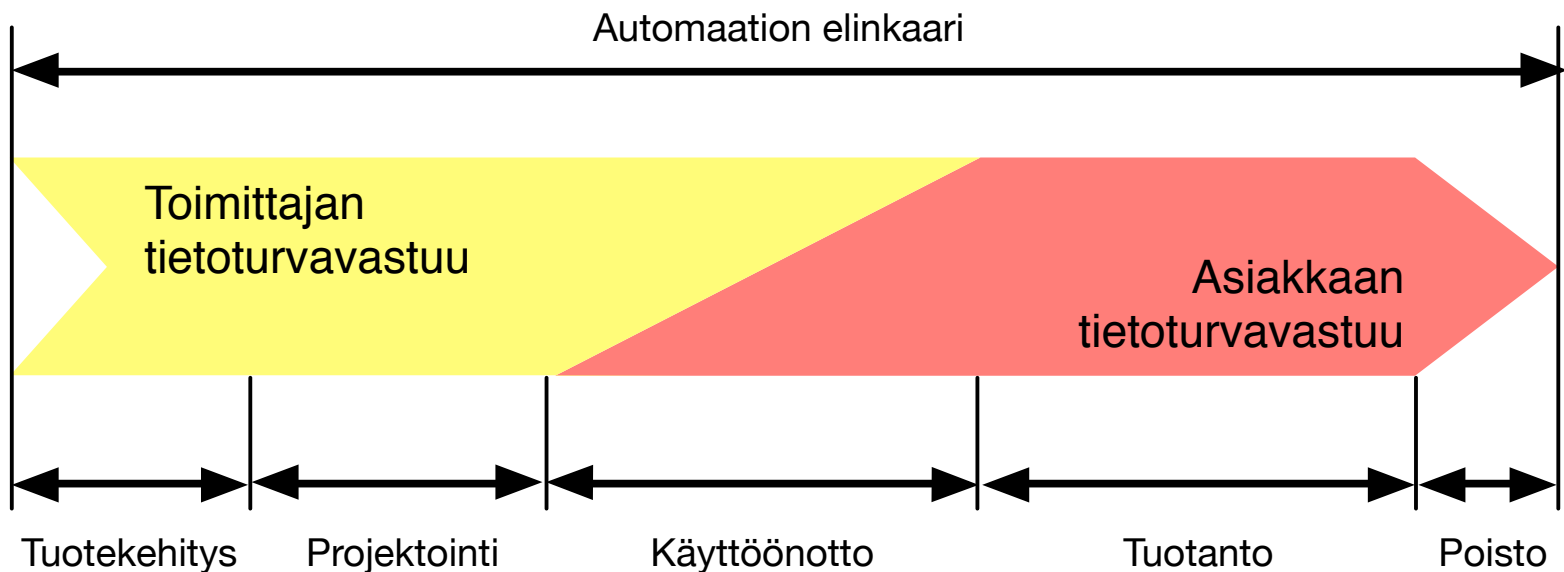
Tietoturva automaation elinkaareissa

- Tietoturva on oleellinen osa **luotettavuuden** parantamista
 - **Turvajärjestelmä** → tahattomat tilanteet (vahingot)
 - **Tietoturva** → tahalliset toimet
- Tietoturvan mekanismit auttavat myös vahinkoihin
 - ”käyttämättömät portit poistettu käytöstä”
- Turvajärjestelmän mekanismit auttavat tietoturvassa
 - Liikennevirheiden havaitseminen
 - Erilliset tietoliikenne- ja ohjelmaprosessorit



Automaation erityispiirre: tietoturvavastuun siirtyminen

- Tieturvan vastuutus ja erityisesti **päävastuun** siirtyminen kuuluu aina kaikkiin automaatioprojekteihin



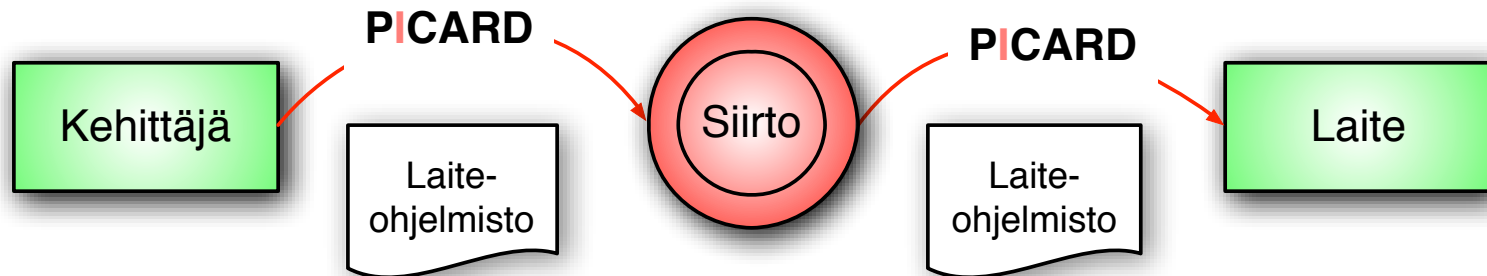
Luotettavan automaation tuottaminen?

1. Mallinna järjestelmä liiketoimintatavoitteen kannalta (mitä)
2. Mallinna käyttötapaukset (miten)
3. Kirjaa ylös toimijat (järjestelmät, ihmiset, ...)
4. Määrittele kuka hallitsee järjestelmää (ohjaus)
5. Määrittele tietoon liittyvät prosessit
6. Määrittele tietovuot
7. Määrittele tietovoiden sisällöt
8. Rakenna *luottavuusmallit* (tietoturva ja automaatio)
9. Valitse suojausmekanismit (kerran mietitty => vain valinta)
10. Toteuta



Luotettavuusmalli (dependability model)

- Tietovuomalli, jossa myös automaatiovaatimukset mukana



P, yksityisyys
I, eheys
C, luottamuksellisuus
A, hälytys
R, reaaliaikaisuus
D, jäljitettävyys

Soveltuu

- keskustelujen pohjaksi sekä
- systemaattiseen tietoturva-analyysiin

Helppo työkalu

- Ei vaadi "järjestelmää" tai "sovellusta"
- Toimii niin järjestelmien kuin raudankin analyysissä



TAMPERE UNIVERSITY OF TECHNOLOGY

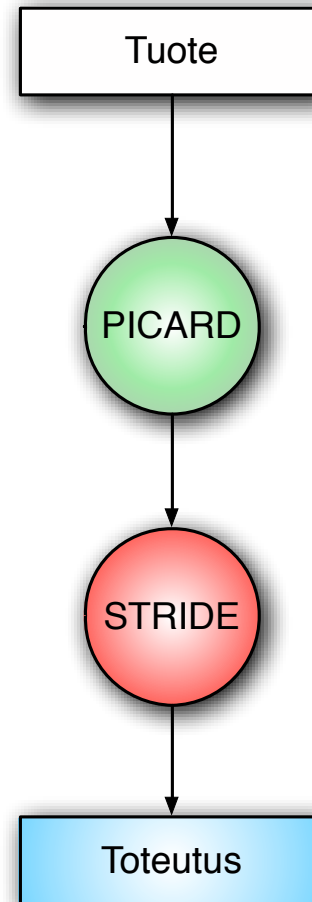
Turvallisen kehittämisen malli (Secure Development Lifecycle)

Uusi tuote, käyttötapaus, tai
sovelluskohde

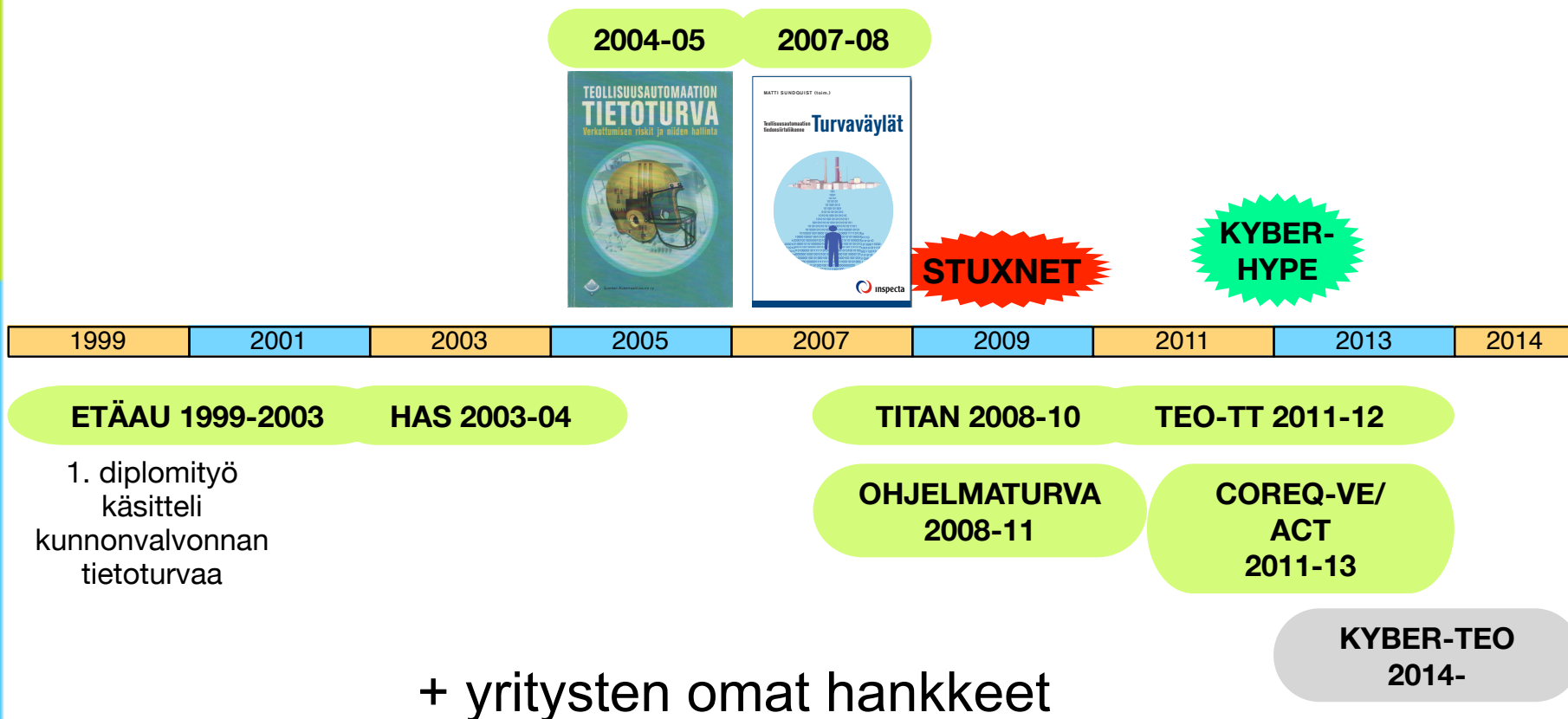
Luotettavuusmalli
- tietovuot
- automaatiovaatimukset
- tietoturva-vaatimukset

Turvallisen kehittämisen elinkaari
- uhat
- uhkien torjunta

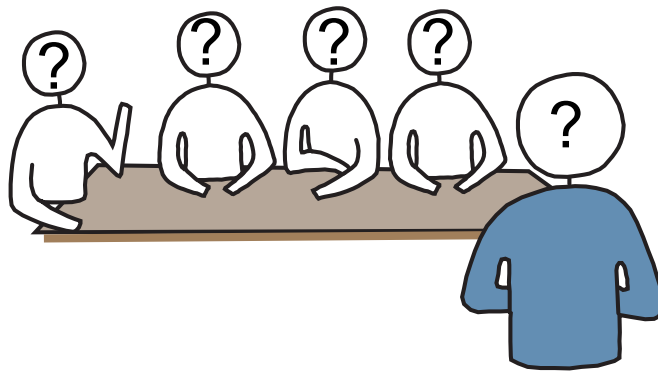
Kehitystyökalut
- toteutukset, ”työkalupakki”



Suomen automaation tietoturvatyön elikaari



Kysymyksiä



Kirjallisuutta

- Kim Paananen: Information Security in Smart Grid Demonstration Environment
 - <http://URN.fi/URN:NBN:fi:tty-201205161123>
- SAS: Teollisuusautomaation tietoturva - verkottumisen riskit
 - <http://www.cert.fi/palvelut/hvk/tietoa/julkaisut.html>
- COREQ-VE/ACT-materiaali
 - pasi.ahonen@vtt.fi

