Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaation kyberturvallisuus

- 4 - Liityntä prosessiin

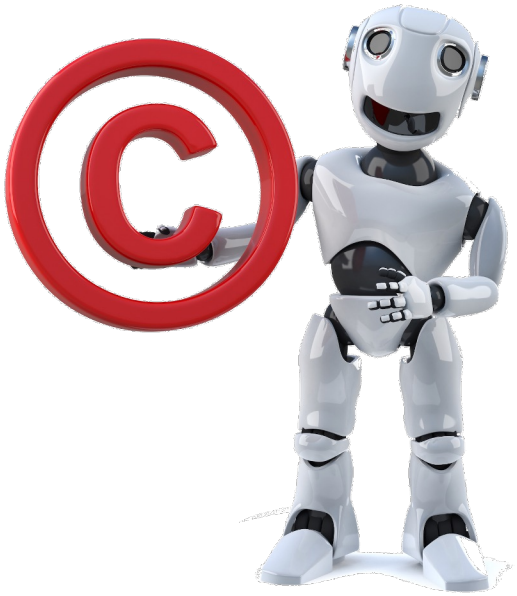
Kyy hanke
Mikko Korpela, Tampereen Ammattikorkeakoulu
Ville Haapakangas, Tampereen Ammattikorkeakoulu

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Materiaalin oikeudet

Kyy –hanke
TAMK

- Materiaali on tehty osana OKM hanketta: *Kyberturvallisuuden opintokokonaisuudet* (Kyy)
- Copyright © *Tampereen Ammattikorkeakoulu; Mikko Korpela, Ville Haapakangas 2025*
- Käytetyt lisenssit :
  - Adobe Stock, Education License, Käytössä TUNI:n kautta
  - MS Powerpoint, Office 365, Käytössä TUNI:n kautta
- Käyttöehto:
  - Materiaalin käyttö sallittu vain opetuskäyttöön
  - Alkuperä mainittava



Kuva: AdobeStock,

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaatiojärjestelmä

Kyy –hanke
TAMK

- Automaatiojärjestelmä jaetaan standardin IEC 62264 mukaan tasoihin
  - Malli pitää sisällään kaikki yrityksen toiminnot

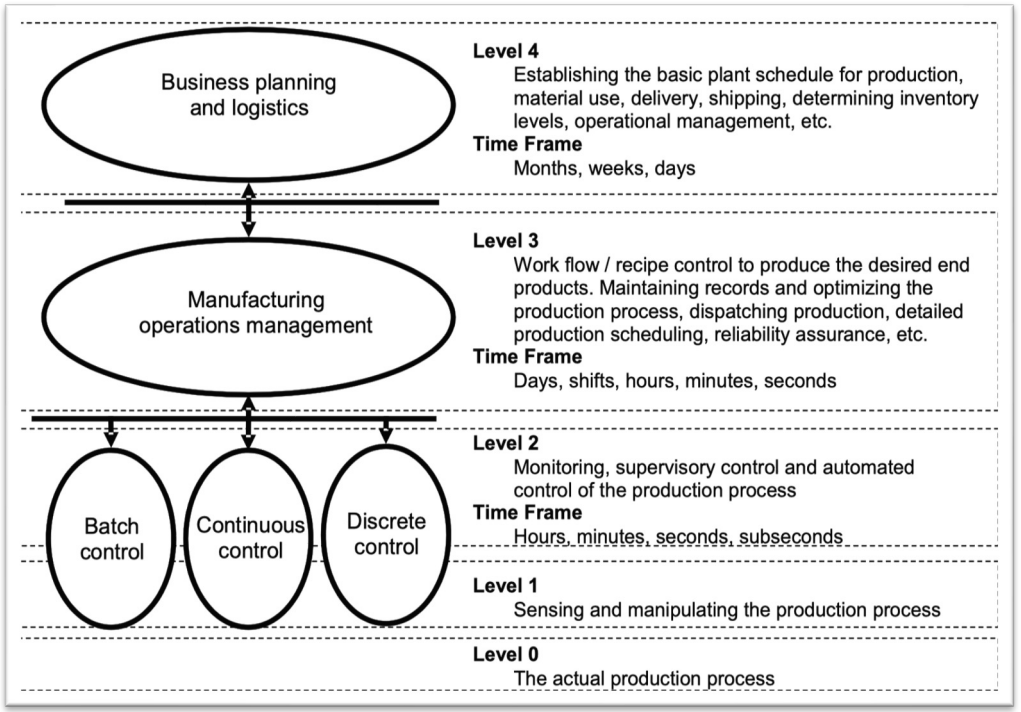
- Taso 4: Toiminnanohjaus (ERP)
  Esim: SAP
- Taso 3: Tuotannonohjaus (MES)
  Esim: LeanwareMES

IT järjestelmä

- Taso 2: Prosessin ohjaus / hallinta (SCADA / DMS)
  Esim: MicroSCADA X
- Taso 1: Kenttäinstrumentointi (Anturit / Toimilaitteet / PLC)
  Esim: Sick, ABB, Siemens

OT järjestelmä

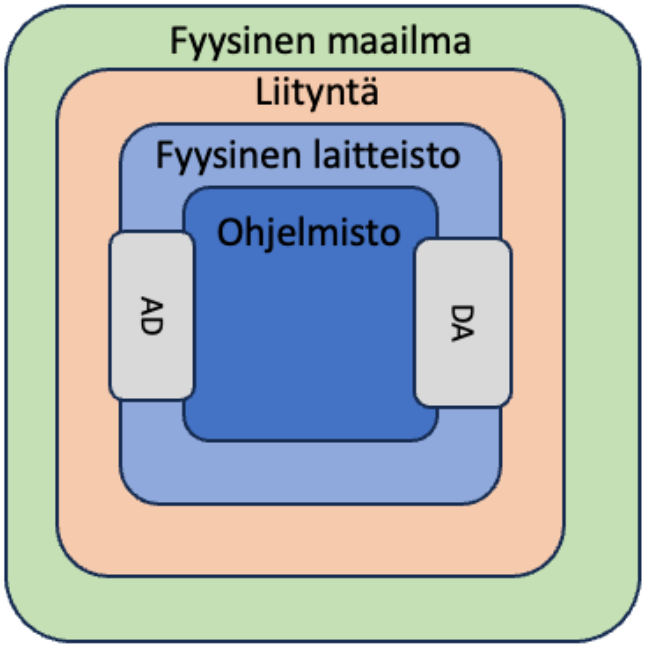
- Taso 0: Prosessi



IEC 62264-1:2013 Figure 3 – Functinal hierarchy

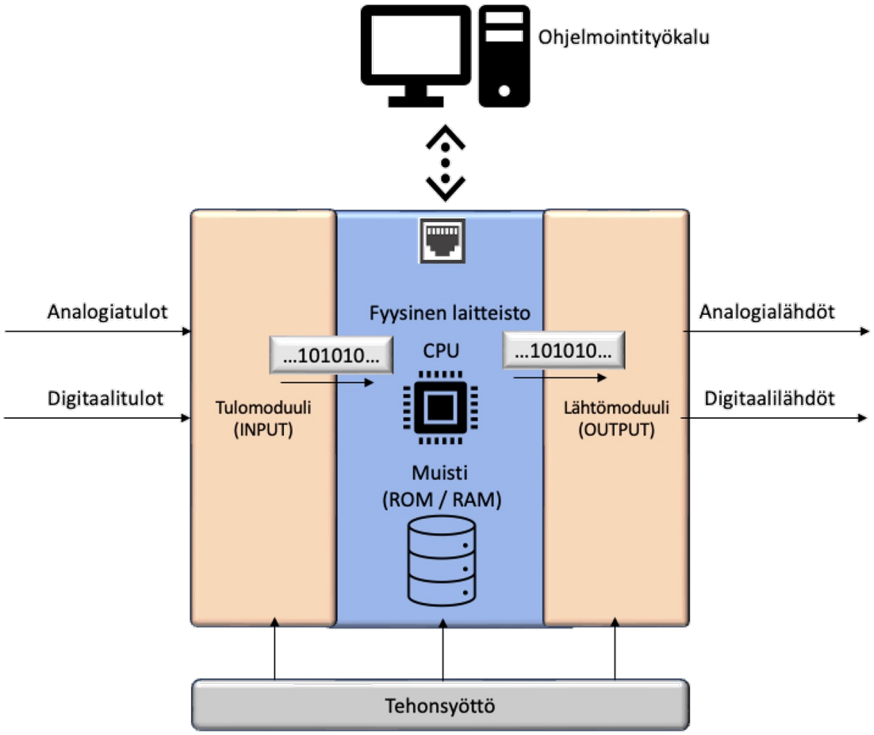
Liityntä prosessiin

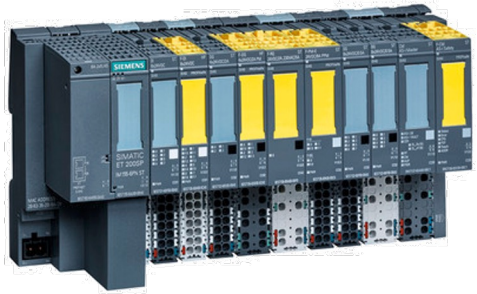
- Tuotantoautomaation kyberympäristö tarkoittaa digitaalisista järjestelmistä koostuva kokonaisuus johon kuuluu:
  - Fyysiset laitteet (Tietokoneet, yksikköohjaimet (PLC), palvelimet, tietoliikenne)
  - Ohjelmistot (käyttöjärjestelmät, sovellusohjelmistot, tiedonsiirto ja käsittely ohjelmistot)
  - Kyberympäristö toteuttaa jotain toiminnallista käyttötapausta (Haluttu toiminnallisuus)
- Kyberympäristöllä on liityntä fyysiseen maailmaan.
  - Fyysisen maailman analoginen tieto muutetaan digitaaliseksi (AD -muunnos)
  - Kybermaailman digitaalinen tieto muutetaan analogiseksi (DA –muunnos)
- Esimerkkejä käytännön liitynnöistä
  - Prosessiliityntä (Toimilaitteet / anturit)
    Esim: moottori ja etäisyysanturi
  - Operaattoriliityntä (Toiminnan ohjaus ja valvonta)
    Esim: käyttöpainikkeet ja ilmaisuvalot
  - Loppukäyttöjäliityntä (Palvelu)
    Esim: verkkopankki



PLC

- Ohjelmoitavat logiikat (PLC) on suunniteltu tehdasympäristöön
  - ”Tietokone”, joka on suunniteltu suorittamaan prosessia
- PLC toimii kovan reaaliaika periaatteen mukaan (reaaliaika käyttöjärjestelmä)
  - Tapahtumat tehdään priorisoiden määrättyjen aikarajojen sisällä. Aikarajan ylitys keskeyttää toiminnan!





Kuva: Siemens

Programmable Logic Controller määritelmä (EN / IEC 61131-1)

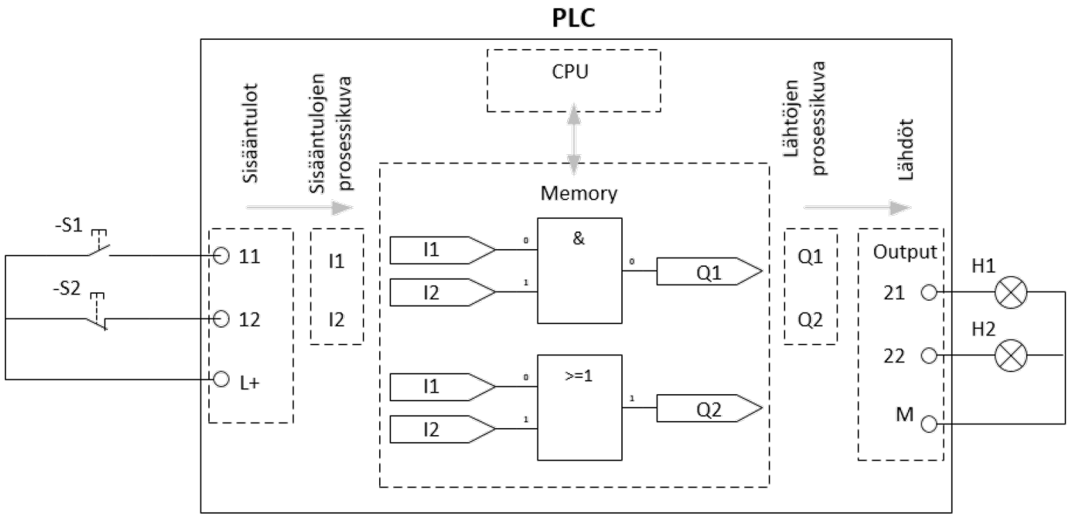
”*A digitally operating electronic system, designed for use in an industrial environment, which uses a programmable memory for the internal storage of user oriented instructions for implementing specific functions such as logic, sequencing, timing, counting and arithmetic, to control through digital or analogue inputs and outputs, various types of machines or processes.*

Both the PC and its associated peripherals are designed so that they can easily integrated into an industrial control system and easily used in all their intended function”

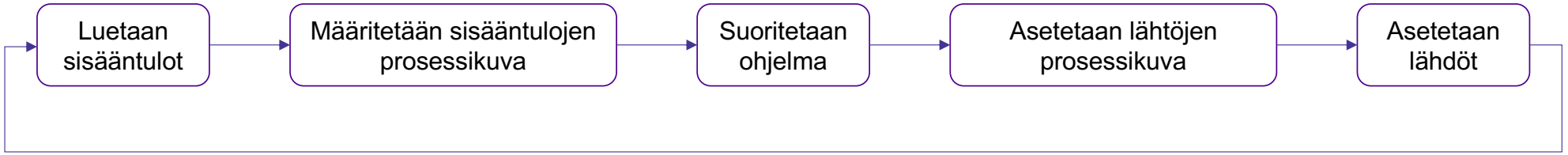
Automaation Kyber-ympäristö

PLC toimii syklisen toimintaperiaatteen mukaan

- Sykli:
  1. Luetaan sisääntulot
  2. Määritetään tulojen prosessikuva
  3. Suoritetaan sovellusohjelma
  4. Asetetaan lähtöjen prosessikuva
  5. Asetetaan lähdöt
- Syklinaika voi vaihdella
  - Erilliset ohjelmalohkot tai laiteyksiköt aikakeskeytyksiin
  - Huomioitava esimerkiksi liikkeen ohjauksessa ja aikariippuvaisissa säätöpiireissä
- Suuritaajuisilla sisääntuloilla tulee huomioida ohjelman kierto
  - Ohjelmakierto 15 ms ⇒ teoreettinen lukutaajuus ~66 Hz
  - HUOM! Syklin aikana sisääntuloja ei lueta!



PLC:n suoritusvaatimukset määritetään ohjattavan prosessin mukaan!



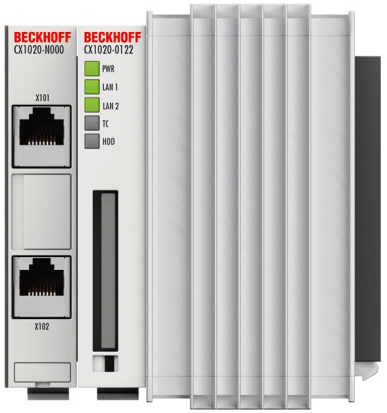
Automaation Kyber-ympäristö

PLC:n tärkein ominaisuus on luotettavuus

- PLC on hyvin lähellä prosessia → aikaikkuna, jonka jälkeen tapahtuma näkyy prosessissa on lyhyt 1 … 500 ms
- Tämän vuoksi PLC on optimoitu suorittamaan sovellusohjelmaa (tehtävää)
- PLC:n resurssit (laskentateho)
  - Esim: Beckhoff CX1020
    - Prosessori: 1 GHz (Intel)
    - RAM: 256 MB
    - OS: Windows Embedded CE 6, Windows Embedded Standard 2009
  - Osassa malleissa resurssit ovat vielä pienemmät.

Huomioitavia seikkoja

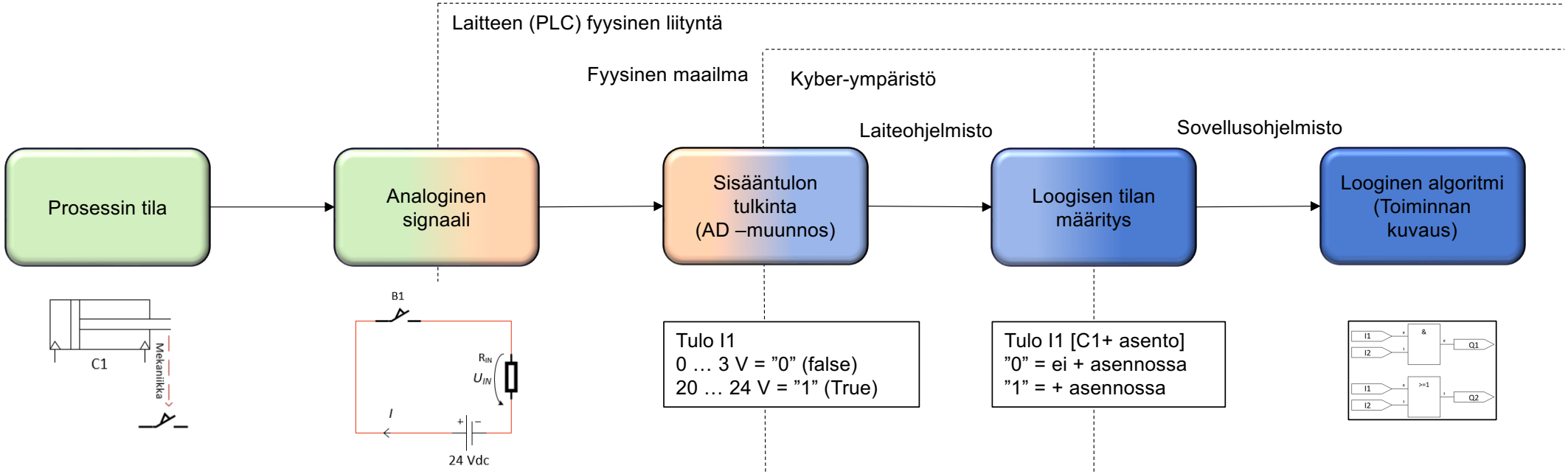
- PLC:n resurssi on pieni, liika kuormitus vaarantaa reaaliaikaisuuden



Kuva: Beckhoff.com

Automaation Kyber-ympäristö

- Kyber-ympäristön liityntä
  - Fyysinen maailma on analoginen / Kyber-ympäristö on digitaalinen
    - Tulevatieto (IN) tulkitaan digitaalisesti (AnalogDigital conversion AD)
    - Lähtevä ohjaus (OUT) muutetaan analogiseksi (DigitalAnalog conversion DA)
- Esim: Digitaalinen tulo (Digital input DI)
  - Sisääntulon tila tulkitaan loogiseksi todeksi tai epätodeksi (1 bittinen AD muunnos)
  - Merkitys tulkita aina prosessin perusteella



Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Kyber-ympäristö

Kyy –hanke
TAMK

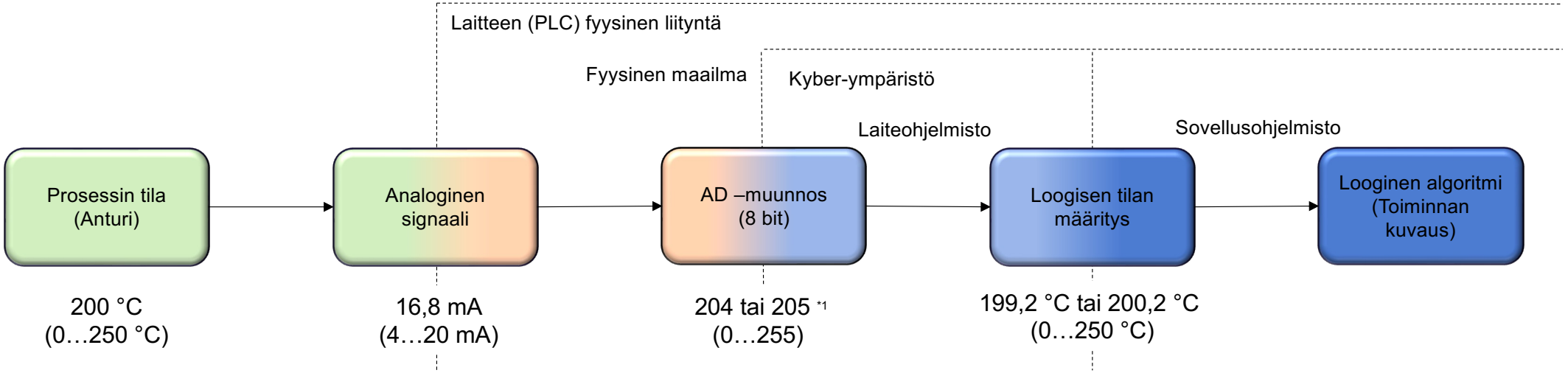
- Analoginen mittaustieto muutetaan kokonaisluvuksi, jonka suuruus riippuu AD muuntimen resoluutiosta
- AD muunnos aiheuttaa epätarkkuutta
  - Esimerkiksi: Lämpötilan mittaus 0 … 250 °
    - 8 bit AD muunnos: Teoreettinen erottelukyky 0,98 C°
    - 10 bit AD muunnos: Teoreettinen erottelukyky 0,24 C°
    - 12 bit AD muunnos: Teoreettinen erottelukyky 0,06 C°
      (HUOM! AD muuntimen todellinen erottelukyky pitää tarkistaa laitteen dokumentaatiosta)
  - Vaadittava erottelukyky ja kokonaistarkkuus riippuu sovelluksesta

*1 riippuu AD muuntimen pyöristyksestä

$$\frac{(16{,}8-4\ mA)}{(20-4\ mA)} \cdot 256 = 204{,}8$$

- Pyöristys ylös → 205
- Pyöristys alas → 204

- Järjestelmän kokonaistarkkuus on osatekijöiden summa.



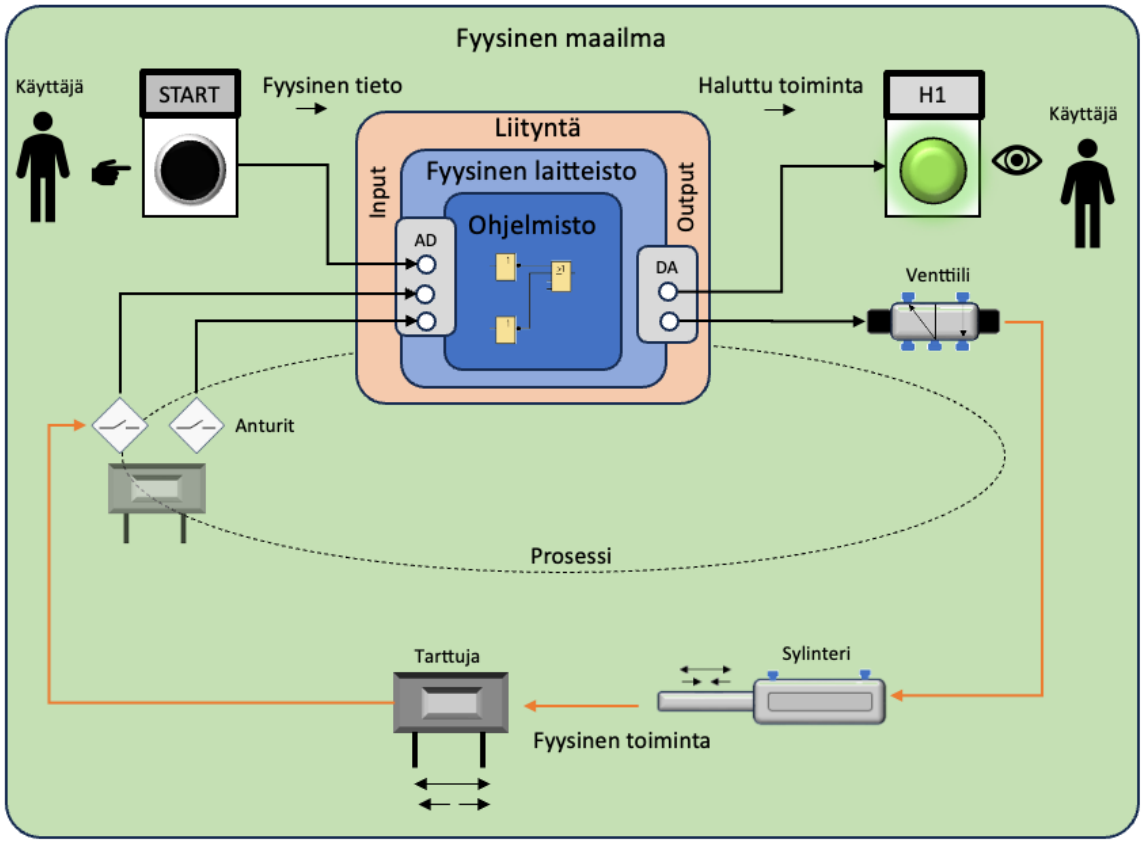
Automaation Kyber-ympäristö

Esimerkki: Sylinterin ohjaus

- Ohjausjärjestelmä suorittaa automaattisesti sille ohjelmoidun tehtävän (Toiminnallisuus)
    - Esimerkiksi tarttujan ohjaus:
        - Tarttuja sulkeutuu, kun käyttäjä painaa painiketta ja avautuu 5 s kuluttua.
        - Valo palaa, kun käyttäjä voi sulkea tarttujan

HUOM! Toiminnallisuus pitää aina tuntea!

- Järjestelmälle viedään (IN) tarvittavat tiedot
    - Painonappi (käyttäjän tahto)
    - Anturit (prosessin tieto)
- Järjestelmä tuottaa (OUT) halutun toiminnallisuuden kannalta tarvittavat tiedot (ohjaukset)
    - Valo (käyttäjän tilatieto)
    - Venttiili (prosessin ohjaus)
- Ohjelmisto (algoritmi) tuottaa loogisen toiminnallisuuden, joka täyttää vaatimukset



Digitaalinen maailma on vain osa kokonaisuutta!

- Myös fyysinen toiminnallisuus pitää tuntea

Kyber-ympäristö

- Tulevasta raakadatasta jalostetaan tietoa, jota hyödynnetään järjestelmässä
  - Raakadatan perusteella on haasteellista tunnistaa vikoja.
  - Esimerkiksi: oikosulku voi johtaa tilanteeseen, että anturin tieto näyttäytyy virheellisenä
  - Päättelemällä tila kahden tiedon perusteella, voidaan parantaa tiedon luotettavuutta

B1	B2	Asema
0	0	Määrittämätön
1	0	+ Asento
0	1	- Asento
1	1	Vika

- Esimerkki: Vika anturin B1 kytkennässä
  - Raakadatan perusteella sylinteri voi olla molemmissa asennoissa yhtä aikaa
    →Mahdoton tilanne