Kyy –hanke
TAMK

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaation kyberturvallisuus

- 5- Automaatioväylät

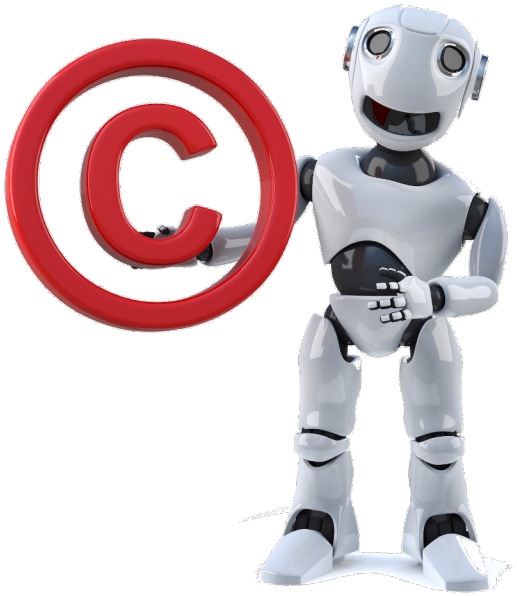
Kyy hanke
Mikko Korpela, Tampereen Ammattikorkeakoulu
Ville Haapakangas, Tampereen Ammattikorkeakoulu

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,

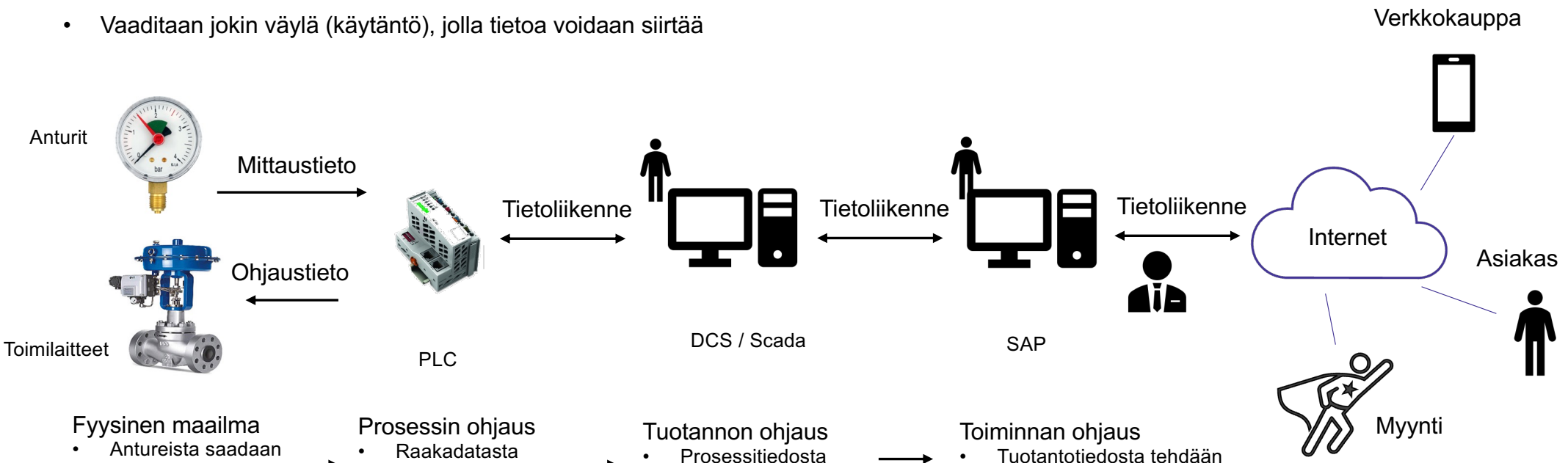
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaatiojärjestelmä

Kyy –hanke
TAMK

Automaatiojärjestelmän pohjana toimii tietoliikenne ja automaattinen tietojen käsittely (ATK)

- Vaaditaan jokin väylä (käytäntö), jolla tietoa voidaan siirtää



Fyysinen maailma
- Antureista saadaan raakadataa
- Toimilaitteilla vaikutetaan prosessiin

Prosessin ohjaus
- Raakadatasta jalostetaan tietoa
- Tiedosta muokataan ohjausarvo

Tuotannon ohjaus
- Prosessitiedosta jalostetaan tuotantotietoa
- Tuotannon vaatimuksista määritetään prosessin ohjausarvot

Toiminnan ohjaus
- Tuotantotiedosta tehdään liiketoimintapäätöksi
- Liiketoimintapäätökset määrittävät tuotannon ohjearvot

Fyysisestä toiminnasta päätöksen tekoon

Päätöksestä fyysiseksi toiminnaksi

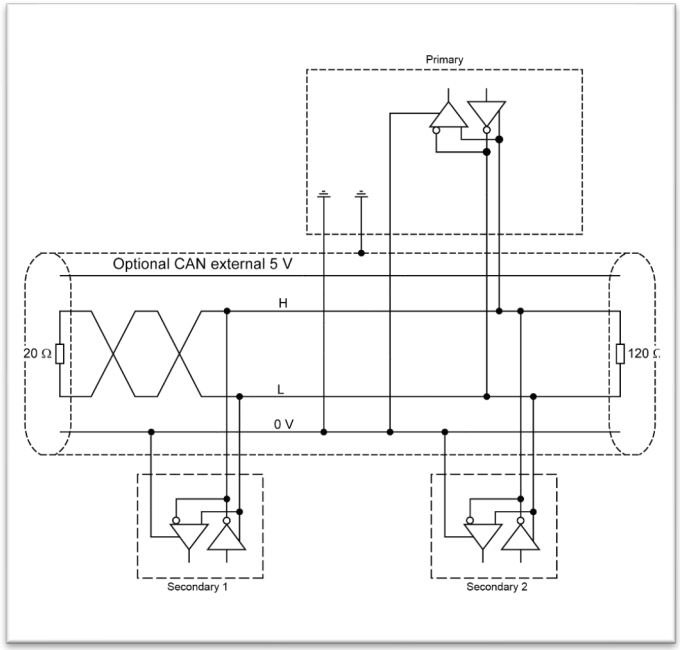
Väylä

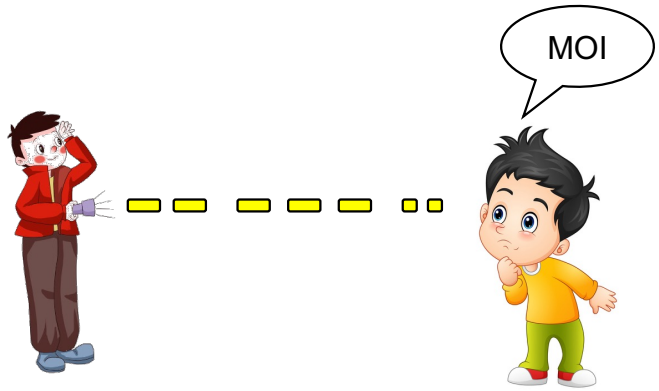
Väylällä tarkoitetaan järjestelmää, joka siirtää tietoa laitteiden tai laitteen osien välillä (informaatioväylä)

- Voidaan yleistää tiedonsiirroksi
- Ei ole välttämättä sähköinen. Tieto voi siirtyä vaikka operaattorin avulla

Fyysiset ratkaisut kertoo miten tietoa siirretään (siirtotekniikka)

- Digitaalisessa tiedonsiirrossa tieto siirtyy bitteinä, mutta siirtotie on analoginen (analogista signaalia tulkitaan digitaalisesti)
  - Rinnakkainen tiedonsiirto. Tieto lähetetään montaa väylää pitkin yhtä aikaa.
  - Sarjamuotoinen tiedonsiirto. Tieto lähetetään yhtä väylää pitkin sarjana





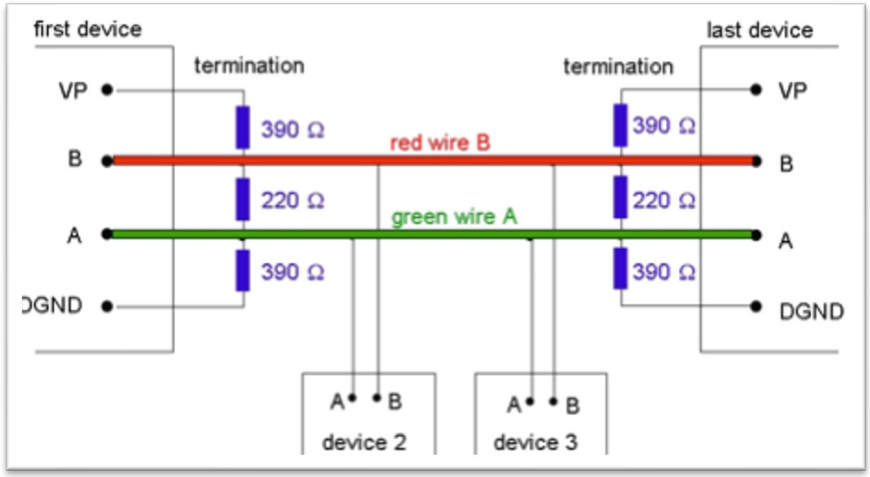
Periaatteellinen CANopen standardi kytkentä
Lähde: Schneider Electric, DOCA0132EN-01 02/2024, s 12,

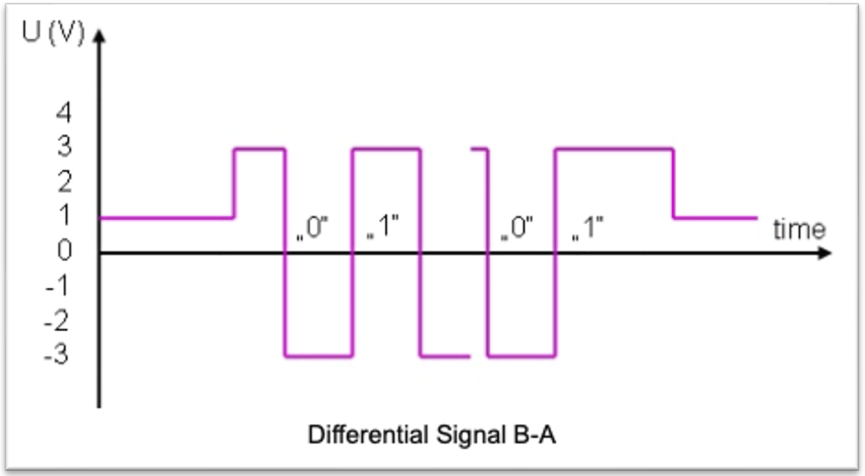
Kuva: AdobeStock, (Muokattu)

Fyysinen siirtotie

Fyysisen tiedon siirtotavan

- Signaalityyppi (valo / sähkö / radio)
  - Fyysinen ilmiö tulkitaan digitaalisesti (looginen 1 tai 0)
- Digitaalinen tiedonsiirtonopeus (bit/s tai byte/s)
- Esim RS485 (Standardi ANSI 485)
  - Signaalitaso -7 V … +12 V
    - Looginen 1 tulkitaan, kunnes $U_A - U_B < -200$ mV
    - Looginen 0 tulkitaan, kunnes $U_A - U_B > +200$ mV
  - Vaatii terminoinnin (päätevastukset)
  - Esim: Profibus DP väylän fyysinen kerros perustuu RS-485 standardiin





Kuvat: https://www.felser.ch/profibus-manual/elektrische_uebertragung.html

Lähde: PROFIBUS System Description

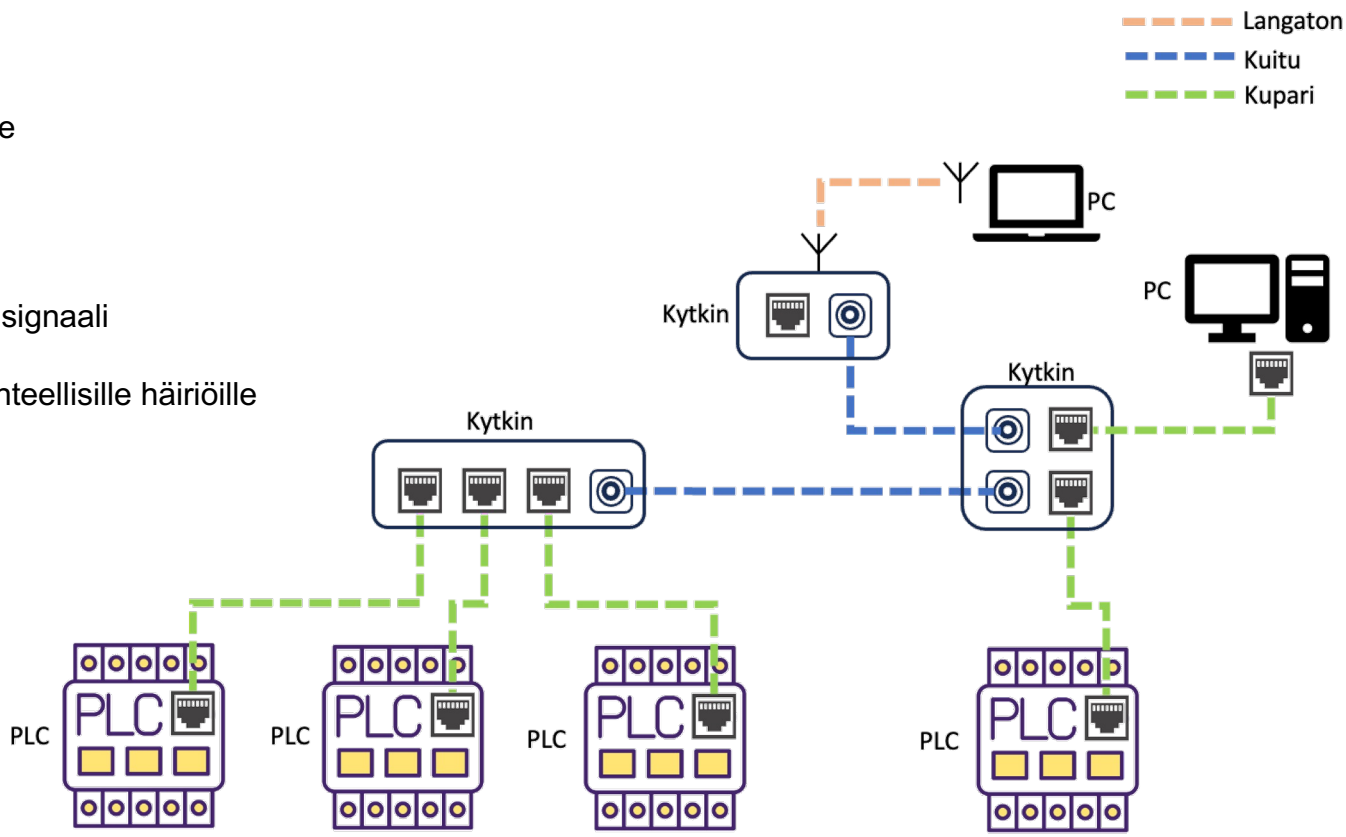
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Fyysinen verkko

Kyy –hanke
TAMK

Fyysinen verkko

- Esittää miten väylän fyysinen siirtotie on rakennettu (kytketty)
- Verkossa voi olla erilaisia fyysisiä tapoja tuottaa signaali (siirtää tietoa)
- Yleiset fyysiset siirtotie
  - Kupari, Sähköinen signaali
    - Helppo liittää ja asentaa
    - Altis sähkömagneettisille häiriöille
  - Kuitu (Fiber), Optinen signaali
    - Hyvä häiriönkesto ja nopeus
    - Mahdollistaa pitkät etäisyydet
    - Haasteellinen asentaa
  - Langaton (radio), Sähkömagneettinen signaali
    - Mahdollistaa hyvän liikkuvuuden
    - Altis sähkömagneettisille ja rakenteellisille häiriöille



Kuva: AdobeStock, (Muokattu)

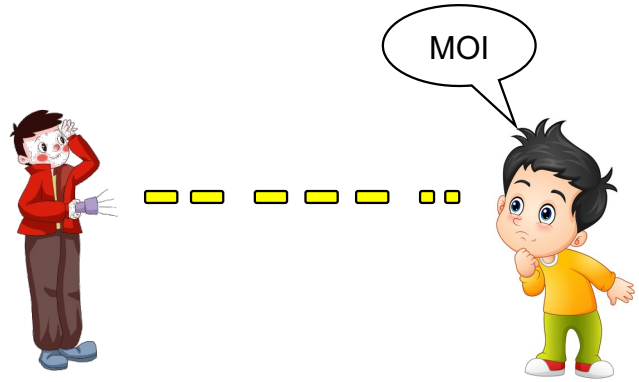
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Protokolla

Kyy –hanke
TAMK

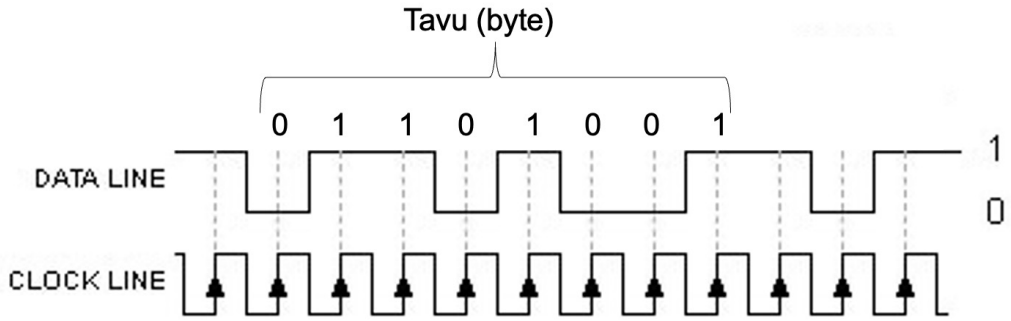
Protokolla(t)

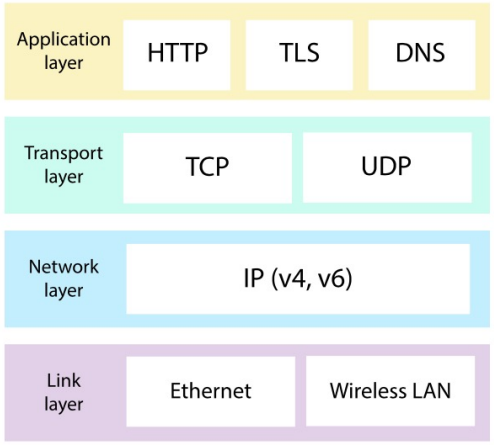
- Yhteiskäytäntö, eli sovittua asia
  - Kertoo miten ohjelmat tai laitteet vaihtavat tietoa
- Esimerkiksi IP protokolla
  - Määrittää miten datapaketti reititetään ja osoitetaan
- Viestin sisältö ja lähetysmuoto pitää sopia (protokolla)
  - Standardit mahdollistavat laitteiden liitettävyyden
  - Esim: USB (Universal Serial Bus)
- Samaa siirtotietä voidaan käyttää eri protokollien siirtoon
  - Esim: Ethercat ja Profinet. Laitteet ”kuulevat” toisensa, mutta ei ymmärrä toisiaan (vrt. Kaksi eri puhekieltä. Sama siirtotie, eri protokolla)



	Protocol Data Unit (PDU)				
Start	Slave ID	Function code	Data	CRC error check	Stop
3.5 Bytes	1 Byte	1 Byte	n Bytes	2 Bytes	3.5 Bytes
	Application Data Unit (ADU)				

Modbus RTU Frame





Internet protokollapino

Kuva: AdobeStock, (Muokattu)
https://community.dataminer.services/question/query-the-parameters-of-a-device-via-modbus/

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Paketointi

Kyy –hanke
TAMK

Esimerkki: Kirjeshakki

- Tiedonsiirto on suorituskyky reaaliaikainen

Lähetys

Lähetys: 2
Saatusiirto: sotilas-E2-E4
Uusi siirto: sotilas-B7-B5

(1/3) Lähetys: 2
(2/3) Saatusiirto: S-E2-E4
(3/3) Uusi siirto: S-B7-B5

Data määritetään mitä halutaan lähettää

Sovellusprotokolla (Segmentointi) Data pilkotaan pieniin sopiviin osiin

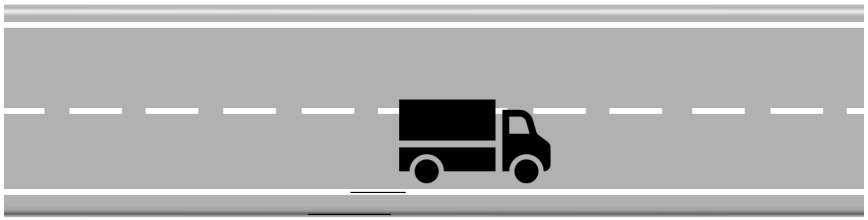
Siirtoprotokolla (Siirtokehys) Data paketoidaan siirtotiehen sopivaksi

Vastaanotto

Lähetys: 2
Saatusiirto: sotilas-E2-E4
Uusi siirto: sotilas-B7-B5

(1/3) Lähetys: 2
(2/3) Saatusiirto: S-E2-E4
(3/3) Uusi siirto: S-B7-B5

Siirtotie



Kuva: AdobeStock, (Muokattu)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Protokolla, OSI malli

Kyy –hanke
TAMK

OSI malli

- Standardimalli, joka mahdollistaa pakettimuotoisen tiedonsiirron erilaisten järjestelmien välillä
- Jakaa tietovirran seitsemään abstratiokerrokseen

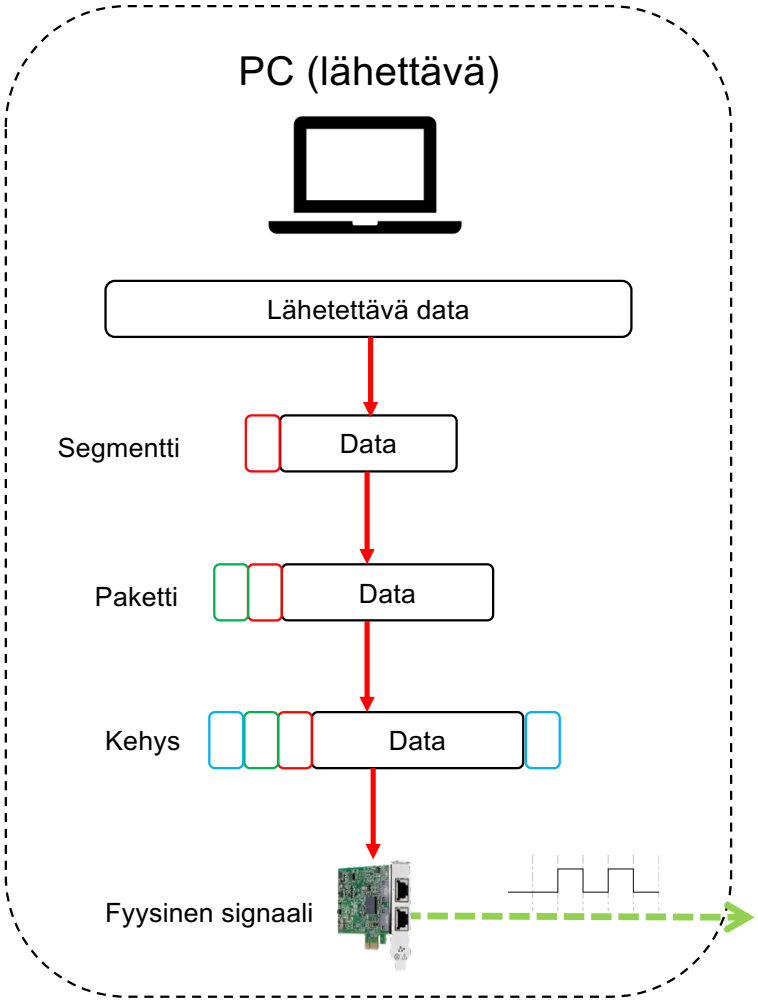
OSI-malli

Kerros		Toiminto	Esimerkiksi
L7	Sovellus	Käyttäjälle näkyvän tiedon hallinta	HTTP
L6	Esitys	Muuttaa tiedon käyttäjälle sopivaan muotoon (esimerkiksi kokoaa kuvan)	.jpg
L5	Istunto	Huolehtii samassa yhteydessä kulkevien eri sovelluksien tiedon kanavoinnista	RPC
L4	Kuljetus (Segmentti)	Huolehtii, pakettien saapumisesta ja niiden järjestyksestä	TCP
L3	Verkko (Paketti)	Tieto minkä laitteiden välillä tieto siirtyy verkossa (Reititys)	IP (v4)
L2	Datayhteys (Kehys)	Linkki kahden laitteen välillä. Määrittää yhteysprotokollan (Kytkin – PC)	Mac address
1	Fyysinen (Analoginen signaali)	Bittivirta ”Raakadata” (Fyysinen laite) Määrittää tiedonsiirron fyysisen median	Sähkö / valo

TCP/IP malli

Sovelluskerros
Kuljetuskerros (Transport)
Verkkokerros (Internet)
Peruskerros Host → Network

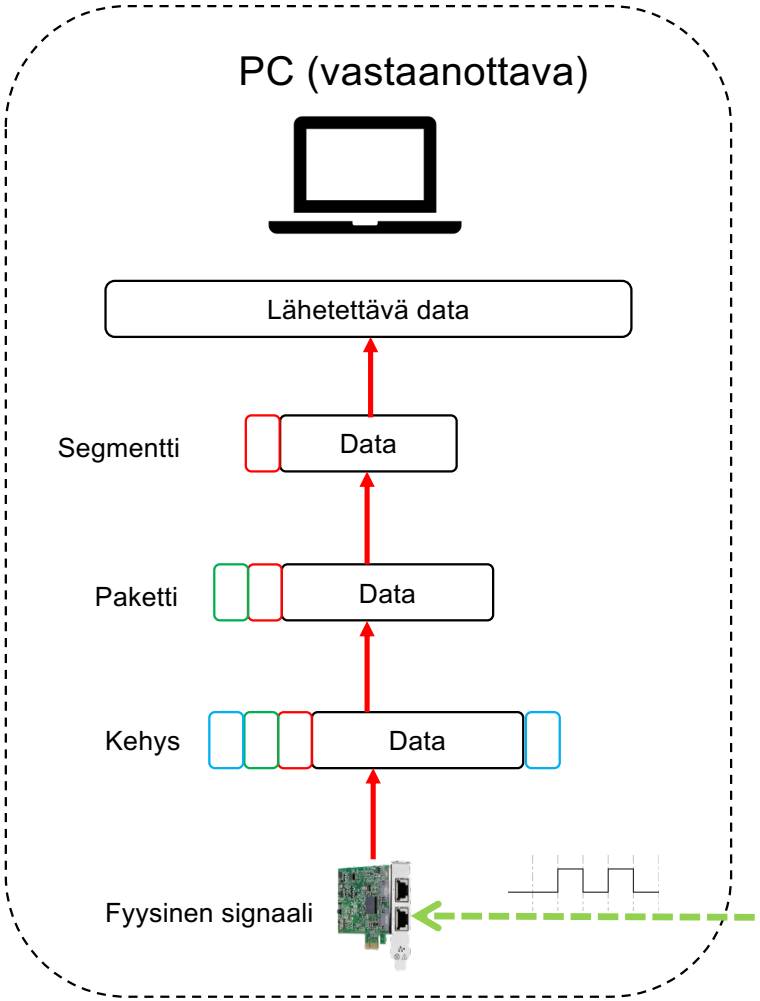
Protokolla, OSI malli



Lähetys:

- Tieto muokataan sovelluksen ymmärtämään muotoon (sovellus) [Sovelluskerros]
- Data pilkotaan sopiviin osiin (segmenteiksi) [Kuljetuskerros]
- Segmentit paketoidaan, eli lisätään lähettäjän ja vastaanottajan tiedot [Internet kerros]
- Paketteihin lisätään kehys, eli lisätään fyysisen siirron tiedot [Verkkoyhteys kerros]
- Kehykset muutetaan fyysiseksi signaaliksi (enkoodaus)

Protokolla, OSI malli



Vastaanotto:

- Kootaan data, jota sovellusohjelma osaa tulkita
- Järjestetään kaikki segmentit ja tarkistetaan, että kaikki paketit on saapunut
- Tarkistetaan kehyksestä, että viesti tuli oikeaan paikkaan ja siirretään seuraavalla kerrokselle
- Erotetaan kehys. Tarkastetaan, että viesti kuului ottaa vastaan ja siirretään seuraavalla kerrokselle
- Fyysinen signaali vastaanotetaan

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaatio Protokollat

Kyy –hanke
TAMK

Automaatioprotokollat

- Erilaiset väylät perustuvat eri standartteihin
- Yleisimpiä väyliä
  - Profinet (Siemens)
  - EtherCAT (Beckhoff)
  - Modbus TCP / IP

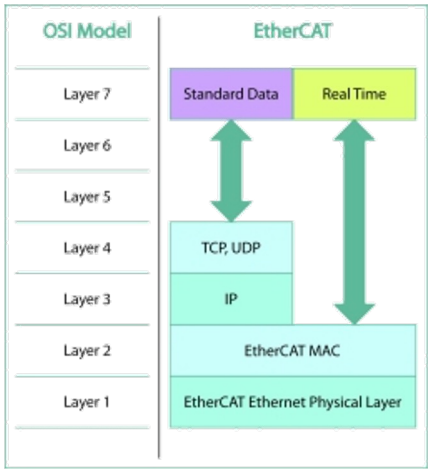
  } Ethernet pohjaisia

  - Profibus
  - Modbus

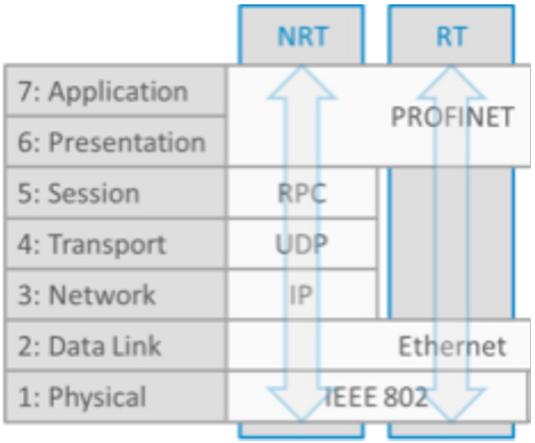
  } RS485 pohjaiset

  - ASI (avoin anturiväylä)
  - KNX (kiinteistöautomaatio)
  - IO –link (anturiväylä)
  - CAN (ajoneuvoväylä)

- Automaatiojärjestelmän erityispiirre on reaaliaikaisuus
  - Tätä vaaditaan myös automaation tietoliikenteen protokollita (Real-Time protocol)
    - Esim: Profinet RT tai IRT
- Erilaiset väylät voidaan yhdistää väylämuuntimien avulla
  - Ei välttämättä ihan helppoa. Saatu tietosisältö pitää purkaa ja rakentaa uudestaan eri protokollan mukaan
  - Käytännössä tehdään protokollamuunnos



Ethercat OSI malli



Profinet OSI malli

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Erilaiset verkot (IT/OT)

Kyy –hanke
TAMK

Automaatiossa reaaliaikaisuus määritetään tiedon hyödyllisyyden perusteella

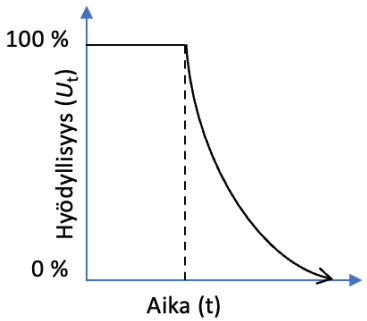
- Ennustettavasti ei välttämättä nopeasti!

Toimistoverkko (IT)

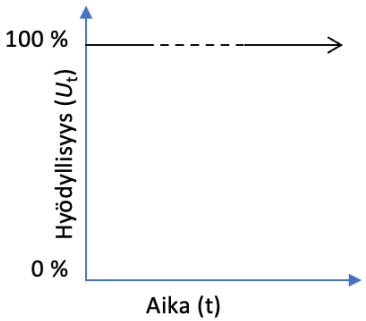
- sallii viiveitä ja pakettien hukkumista (best effort)
  - Mahdollisimman nopeasti, mutta ”toimitusaika” saa vaihdella
- Tiedon saatavuuden estyminen ei aiheuta yleensä merkittävää haittaa prosessille
  - ”Tulostin ei vaan toimi, yritetään uudestaan”
- Verkossa on myös ei niin oleellista dataa
- Ympäristön tyypilliset piirteet
  - jatkuvat pienet päivitykset, ohjelmat ajan tasalla, kriittiset välittömästä
  - Laitekanta vaihtuu tiheästi (5 – 10 vuotta).
  - Laitteilla suuret resurssit / Luetettavuus heikko

Automaatioverkko (OT)

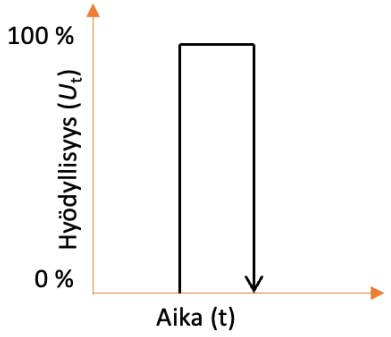
- Synkroninen liikennöinti (Reaaliaika)
  - kova reaaliaikaisuus
  - Isokrooninen reaaliaikaisuus
- Tiedon saatavuuden estyminen voi ”räjäyttää tehtaan”
  - Tai ainakin pysäyttää tuotannon
- Kriittiselle tiedolle tärkeätä tiedon oikeellisuus ja eheys
  - Tietoa on vähän, mutta (lähes) kaikki on oleellista
- Ympäristön tyypilliset piirteet
  - Päivitys (myös ohjelmistojen) suunnitellusti huoltokatkon yhteydessä (esim: 1 kertaa vuodessa)
  - Kaikkia haavoittuvuuksia ei voi korjata, niiden kanssa pitää elää
  - Laitteiden elinaari on pitkä 25+ vuotta
  - Laitteiden pienet resurssit / Luotettavuus hyvä



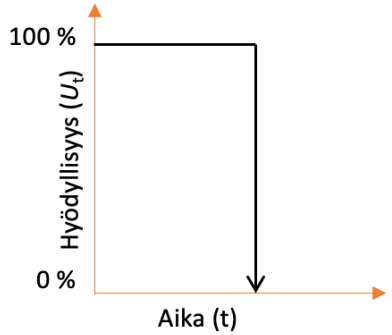
“Best Effort -reaaliaikaisuus



Pehmeäreaaliaikaisuus



Isokroninenreaaliaikaisuus



Kovareaaliaikaisuus

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaatio Protokollat

Kyy –hanke

Esim: Profinet RT ja Profinet NRT erot

Profinet RT (realiaika Protokolla)
- Käytetään automaation prosessiteitojen siirtoon (Esim: Hajautus IO luku / kirjoitus)
- Liikennöinti L2 tasolla → Liikennettä ei voi reitittää

Profinet NRT (Ei realiaika Protokolla)
- Käytetään automaation kannalta ei kriittisen tiedon siirtoon. (Esim: sovellusohjelman siirto)
- Liikennöinti L4 tasolla → Liikennettä voidaan reitittää

Huomioitavaa
- Profinet RT ja NRT käyttää samaa fyysistä siirtotietä
- Kaikki verkkolaitteet (esim: kytkimet) eivät osaa käsitellä reaaliaikaprotokollaa.

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

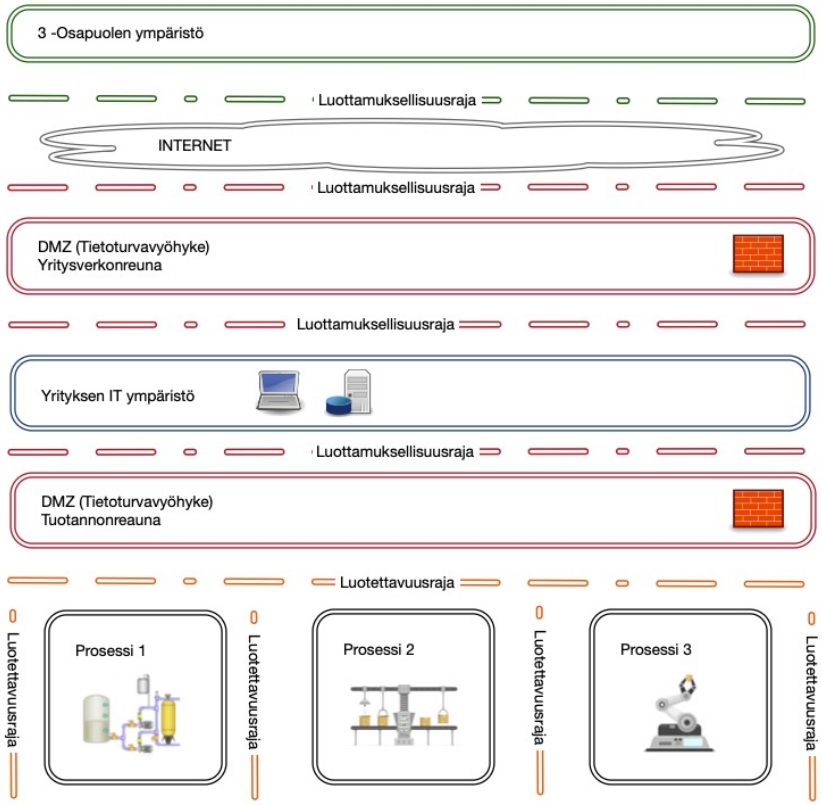
Looginen verkko

Kyy –hanke
TAMK

Verkkoympäristöt jaetaan toiminnallisiin kerroksiin

- Looginen verkko ei ota kantaa miten verkko on fyysisesti rakennettu

- 3-OSAPUOLEN ympäristö
  - Toiminnallisuus: Ei voi määrittää
  - Kuvaus: Ympäristö, johon ei ole mahdollista vaikuttaa
- INTERNET
  - Toiminnallisuus: Yhdistää verkkoja
  - Kuvaus: ”vihamielinen” ja turvaton. Ei voida luottaa mihinkään
- YRITYKSEN REUNA (DMZ tietoturvavyöhyke)
  - Toiminnallisuus: Suojaa yrityksen verkkoa
  - Tehtävä: Liikenteen kontrolli ja seuranta
- TOIMISTOVERKKO
  - Toiminnallisuus: Verkon ylläpito, Yhteiset palvelut
  - Tehtävä: Mahdollistaa yrityksen tietojärjestelmien toiminta
- TUOTANNON REUNA (DMZ tietoturvavyöhyke)
  - Toiminnallisuus: Suojaa yrityksen tuotantoverkkoa
  - Tehtävä: Liikenteen kontrolli ja seuranta
- TUOTANTOVERKKO
  - Toiminnallisuus: ”Ydinprosessi” (voidaan eristää ”kuplaksi”)
  - Tehtävä: mahdollistaa tuotannon
- LUOTTAMUKSELLISUUSRAJA
  - Toiminnallisuus: Erottaa luotettavan ja epäluotettavan ympäristön
- LUOTETTAVUUSRAJA
  - Toiminnallisuus: Erottaa epävakaan ja vakaan ympäristön (Luotettavuus määritetään prosessin perusteella)



Lähde: ISA99/IEC-62443 (värit 62443:n mukaiset)
Jari Seppälä TUNI (jari.seppala@tuni.fi)

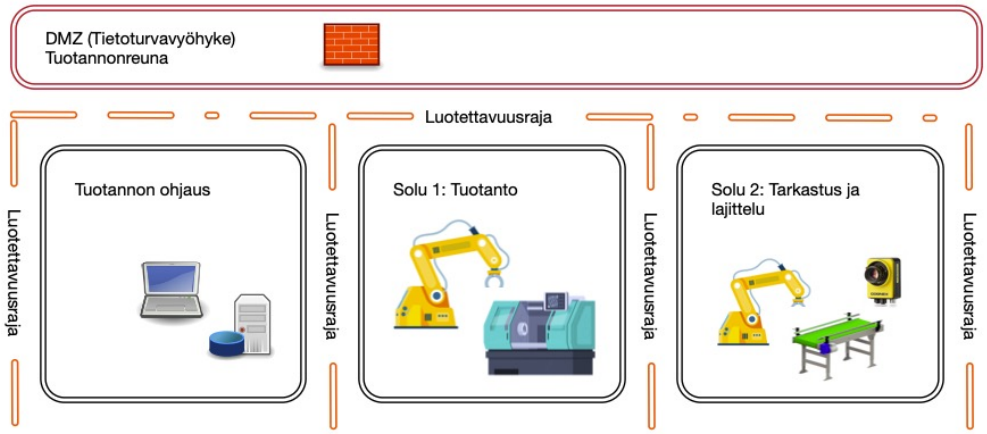
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Looginen verkko

Kyy –hanke
TAMK

Tuotantoympäristön segmentointi

- Tuotantoympäristö on tuotannon jatkuvuuden ja –tiedon kannalta tärkein suojattava ”kriittinen” kohde
  - OT ympäristön ohjelmistoilla voidaan saada aikaan fyysistä tuhoa!
- Segmentoinnin tavoitteena on parantaa ympäristön turvallisuutta ja hallittavuutta
  - Osiin jaettuun ympäristöön on haastavampaa tunkeutua (vrt. fyysisentilan väliovet laitetaan kiinni ja lukkoon)
  - Voidaan hallita tarkemmin tiedonkulkua ja rajoittaa häiriöitä (Muista! Tekniikka mene aina rikki!)
- Kaiken keskiössä on ympäristön tunteminen
  - Pakollinen vaatimus!
- Segmentointi voidaan tehdä ympäristön toiminnallisuuksien tai tietovirtojen mukaan. Esim:
  - Jokainen tuotantosolu on oma segmentti (toiminnallinen)
  - Laitteet, joiden välillä liikkuu tietoa, muodostaa solun (tietovirran mukaan)



Kuva: AdobeStock, (Muokattu)

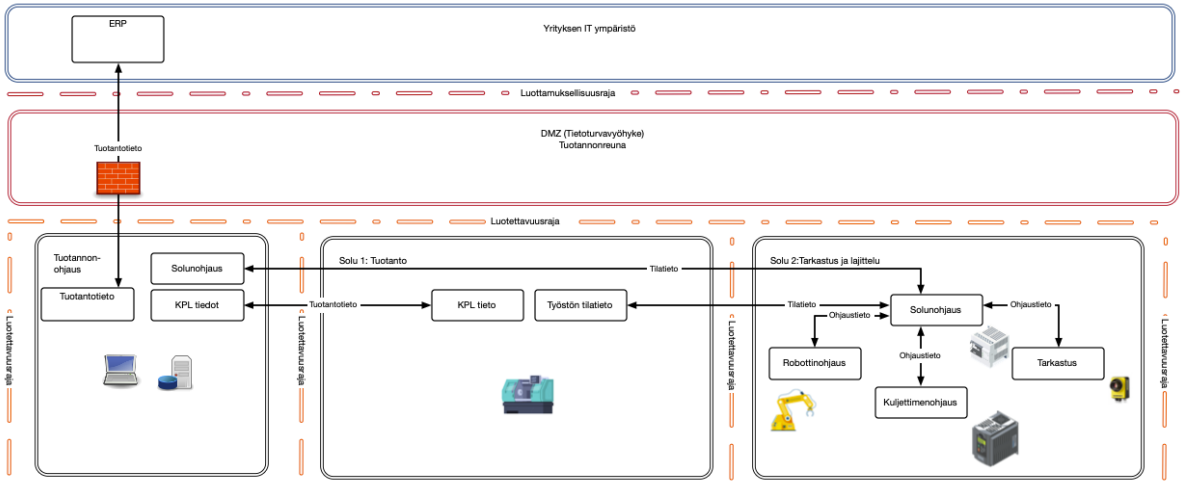
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Looginen verkko

Kyy –hanke
TAMK

Tuotantoympäristön segmentointi

- Esimerkki tuotantoympäristön loogisesta verkosta
- Jokainen solu pystyy tuottamaan oman tehtävän turvallisesti vaikka muut segmentit tai yhteyden menetetään
- IT verkosta ei ole suoraa yhteyttä tuotantolaitteisiin
- Loogisen verkkokuvauksen tarkoitus on ilmaista fyysisen verkon ja verkkorakenteiden vaatimukset



Kuva: AdobeStock, (Muokattu)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

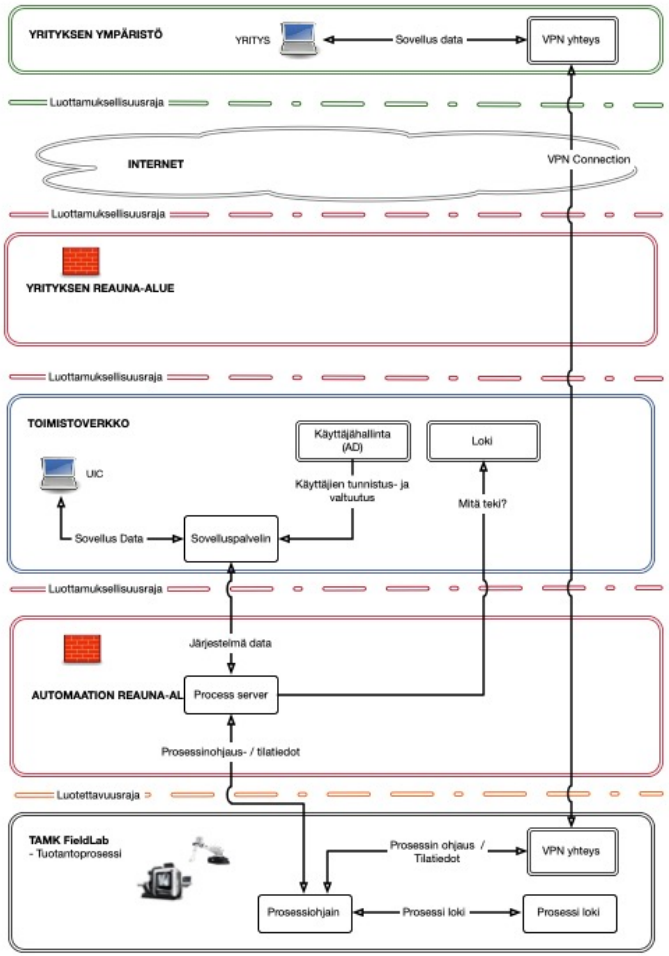
Looginen verkko

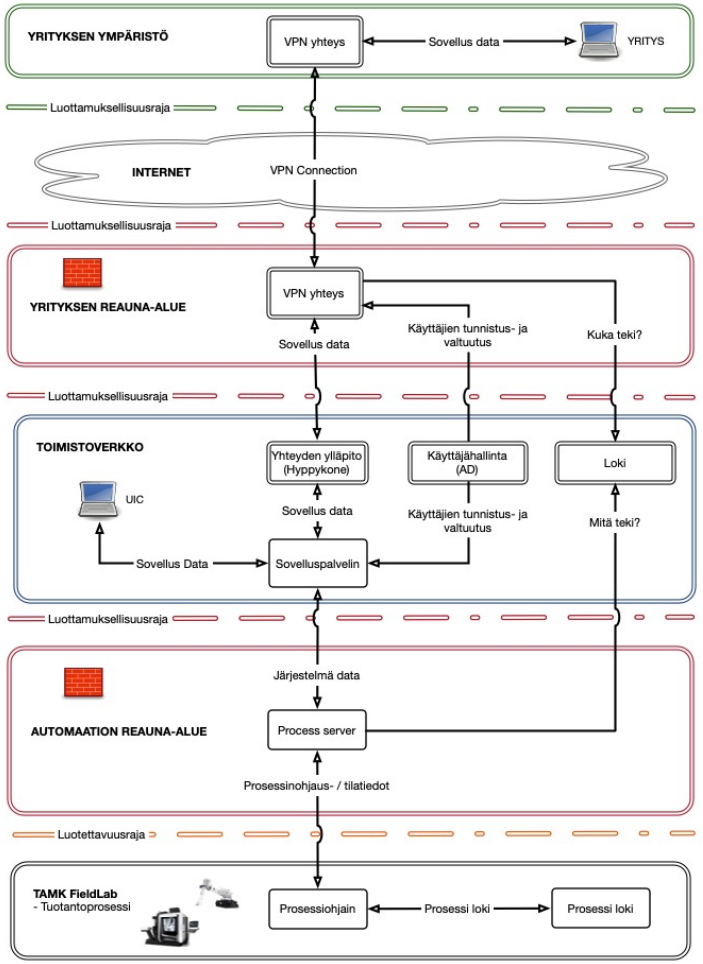
Kyy –hanke
TAMK

Esimerkki: VPN yhteys

- Suora VPN yhteys tuotantoverkkoon
  - Liittää tuotantoverkon 3 –osapuolen verkkoon
    (Ei mahdollisuutta vaikuttaa)
  - Ei kontrollia mitä tietoa liikkuu

- Hallittu VPN yhteys tuotantoverkkoon
  - VPN yhteys kulkee vain Internetin yli
  - Mahdollistaa yhteyden hallinnan ja kontrolloinnin





Kuva: AdobeStock, (Muokattu)