Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Automaation kyberturvallisuus

## - 7- Turvallisuus

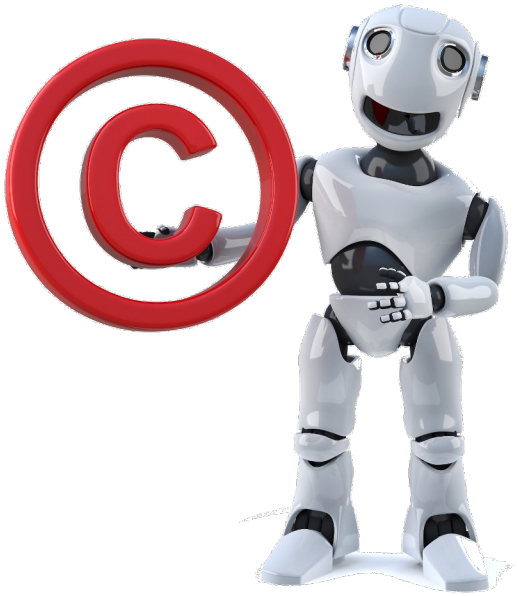
Kyy –hanke, Syksy 2025
Mikko Korpela, Tampereen Ammattikorkeakoulu
Ville Haapakangas,

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

# Tuotantoympäristö

Kyy –hanke
TAMK

Monitoimijaympäristö, kukaan ei osaa kaikkea…

- Tuotannon kokonaisuus koostuu osa-alueista
  - Johto: Periaatteet ja resursointi
  - Hallinto: Toimintaedellytykset
  - Tietoliikenne: Tiedonsiirto
  - Automaatio: Tuotannon ohjaus
  - Prosessi: Fyysinen tuotantoprosessi
  - Operaattori: Tuotannon valvonta
  - Kunnossapito: Tuotannonylläpito
- Onnistumisen kulmakivet
  - Kommunikointi
  - Verkostoituminen
  - Suunnittelu ja dokumentointi
  - Selkeä vastuuttaminen
- Turvallisuus on osa-alueiden tulos
  - Jokainen osa alue vastaa turvallisuudesta osaltaan


Kuva: AdobeStock (Muokattu)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

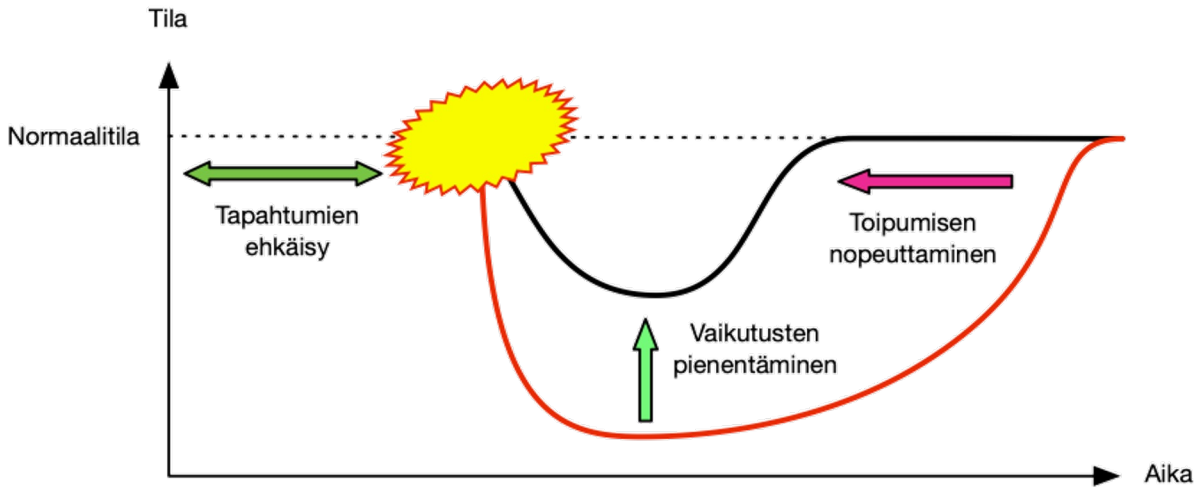
# Tietoturva rooli

Kyy –hanke
TAMK

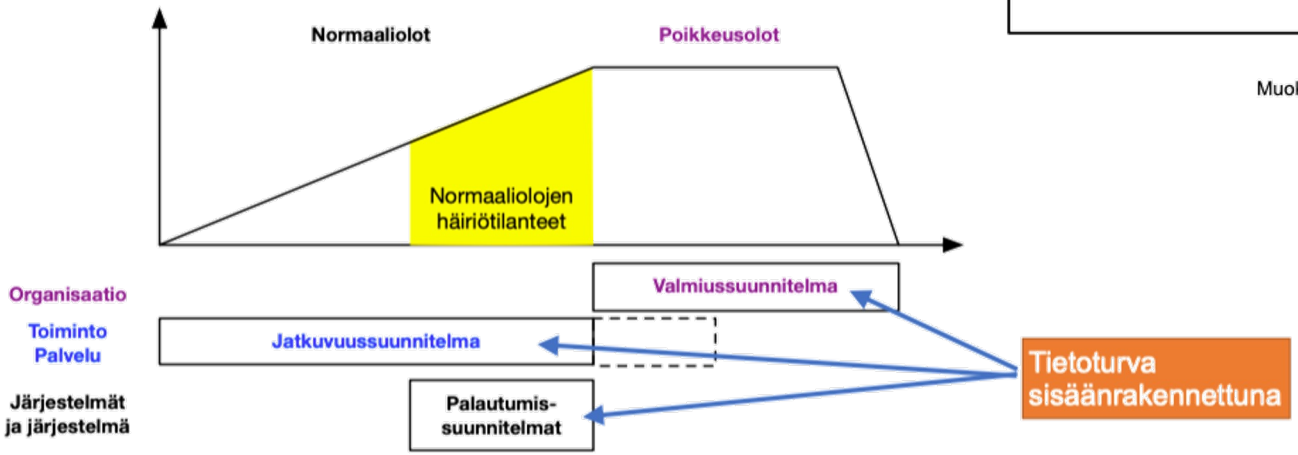
Tietoturvan rooli on

- nopeuttaa toipumista
- Pienen vaikutuksia

Toiminnan keskiössä on jatkuvuuden hallinta




Muokattu lähteestä: Huoltovarmuuskeskus




Lähde: Jari Seppälä. jari.seppala@tuni.fi
Kuva: Jari Seppälä jari.seppala@tuni.f

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Huoltovalmuus

Kyy –hanke
TAMK

Valmistautumista siihen, ~~jos~~ kun jokin resurssi menetetään

- Kone- ja tuotantoautomaatiossa häiriötilanteet ovat osa normaalia toimintaa
  - Insinööri fakta. Kaikki menee rikki
  - Palautuminen häiriötilanteista riippuu siitä miten niihin on varauduttu

Ympäristön tunteminen luo pohjan päätöksenteolle

- Riskien arviointi vaatii, että ymmärtää vaikutukset
- Hyvä ja nopea palautuminen häiriötilanteista ei ole tuuria vaan tietoinen päätös

Harjoittelun avulla onnistumiseen

- Skenaarioharjoitukset avaavat silmiä
- Harjoituksissa epäonnistuminen ei pysäytä tuotantoa

Kuva: AdobeStock, (Muokattu)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Fyysinen turvallisuus

Kyy –hanke
TAMK

## Fyysinen turvallisuus

- Tietoverkon rajoituksilla ja kontrolleilla ei ole apua tuotantotilan fyysiseen lukitukseen
    - Ei tarvitse murtautua verkon kautta, jos voi kävellä sisälle
- OT-ympäristö on altis häiriöille ja poikkeaville tilanteille
    - Reaaliaikaisuus häiriintyy → tuotanto pysähtyy

Esimerkki:

- OT verkkoon kytketään laite, joka lähettää broadcast liikennettä
    - Liikenne kuormittaa kytkimiä, joka aiheuttaa viivettä liikenteeseen
    - Reaaliaikaisuus häiriintyy

Vahinko tai tahallinen → Samalopputulos → Tuotanto häiriintyy

Työkaluja

- Koventaminen! Estetään liikennöinti porteista, joita ei tarvita
- Dokumentointi! Selkeä missä järjestyksessä kytketään

Huomioi ympäristön fyysinen lukitus ja valvonnasta

Kuva: AdobeStock,

# Fyysinen turvallisuus



Esimerkki: Texsasin liikenneviestintä, 2009

- Tammikuussa 2009 Texasin liikenteenohjaustauluihin ilmestyi erikoisia viestejä
- Tapaus aiheutti hämmennystä
- Miksi näin tapahtui
    - Laitteiden ohjaimissa oli oletussalasanat
    - Laitekaapit eivät olleet lukittu

Mitä opitaan

- Kokonaisuus pitää huomioida
- Vastuut pitää määrittää
    - Kuka määrittää / ylläpitää salasanoja
    - Kuka huolehtii lukituksesta
    - Kuka tarkastaa ja vastaa kokonaisuudesta


Lähde: FoxNews, 29.1.2009
Jari Seppälä, TUNI
Kuva: Wired (https://www.wired.com/2009/02/austin-road-sig/)

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Haittaohjelmat

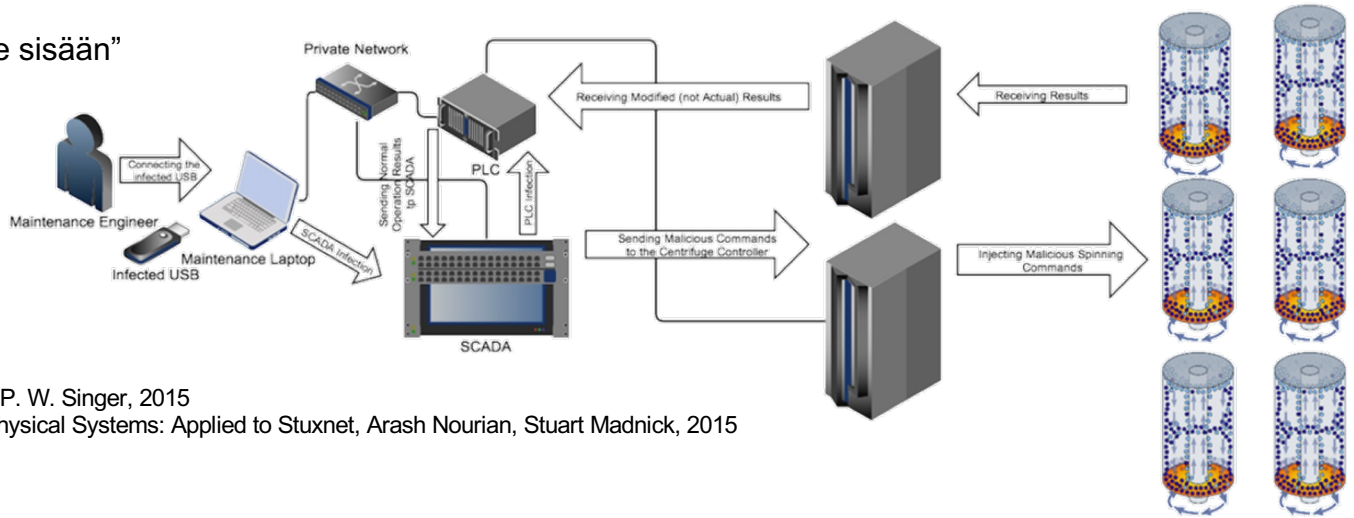
Kyy –hanke
TAMK

## Haittaohjelmat voivat aiheuttaa fyysistä tuhoa

- Stuxnet on haittaohjelma, jonka tarkoitus oli rikkoa OT järjestelmän avulla fyysistä laitteistoa
  - Levisi USB tikun välityksellä (mato)
  - Tunnisti onko ohjausjärjestelmä oikeanlainen
  - Kun löysi halutun laitteiston, muutti ohjelma sentrifugeja käyttävää ohjausarvoa ja rikkoi ne
  - Ohjelma pyrki peittämään toimintaansa vääristämällä valvomon tietoja
- OT järjestelmään kohdistuva haittaohjelma on harvinainen
  - Hyvin vaikea tehdä, koska fyysinen prosessi ja järjestelmä pitää tuntea
    - Helpompaa hyökätä verkkokytkimeen ja rikkoa reaaliaikaisuus!
  - Yleensä hyvin

Eristetty verkko (air gap) ei auta, jos mato ”kävelee sisään”

- Muista peruskäytänteet!




Lähde: Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons, P. W. Singer, 2015
Kuva: A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems: Applied to Stuxnet, Arash Nourian, Stuart Madnick, 2015

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Haittaohjelmat

Kyy –hanke
TAMK

## Haittaohjelmat voivat aiheuttaa fyysistä tuhoa

- 2016 Ukrainan energiaverkkoa vastaan hyökättiin (CrashOverride)
  - Kohdistui sähköverkon valvontaan (Scada) järjestelmään
  - Hyökättiin hyödyntäen teollisuusprotokollia (mm. OPC, MMS/Goose)
  - Tarkoitus tuhota ja häiritä sähkönjakelua

- Suojautuminen on haastavaa, kun motiivi on poliittinen (ei rahallinen)
  - Hyökkääjällä on huomattavan suuret resurssit
- Perusasiat kuntoon:
  - Harjoittele ja tunne ympäristösi
  - Varaudu! Miten toimitaan, kun automaatio ei toimi
  - Huolehdi pääsynhallinnasta
  - Segmentoi
  - Huolehdi reaaliaikaisesta valvonnasta ja lokituksesta

Lähde: A Case Study of the CRASHOVERRIDE Malware, Its Effects and A Case Study of the CRASHOVERRIDE Malware, Its Effects and Possible Countermeasures, Samuel Rector Dragos (https://nsarchive.gwu.edu/sites/default/files/documents/3869008/Dragos-CRASHOVERRIDE-Analyzing-the-Threat-to.pdf)
Kuva: Dragos.com

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

# Haittaohjelmat

Kyy –hanke
TAMK

Ydinvoimala. Yhteys turvajärjestelmään menetettiin

- Vuonna 2003 David-Bessen ydinvoimalan prosessiverkkon iski Slammer virus
  - SPDS (Safety Parameter Displey System) saastui
- Vaikutukset:
  - Yhteys SPDS turvajärjestelmään menetettiin noin 5 h ajaksi
  - Yhteys prosessitietokoneisiin menetettiin noin 6 h ajaksi
- Onneksi ei tullut fyysisiä vahinkoja
- Syynä oli konsulttiyhtiön toimistoverkko, joka oli suorassa yhteydessä prosessiverkkoon ohittaen kaikki palomuurit
- Mitä tapauksen jälkeen tehtiin
  - Parannettiin palomuureja
  - Parannettiin ulkoistenyhteyksien dokumentointia ja toteutustapaa

SUUNNITTELE ja vaadi, että niiden mukaan toimitaan!

Lähde: UNITED STATES NUCLEAR REGULATORY COMMISSION OFFICE OF NUCLEAR REACTOR REGULATION WASHINGTON, DC 20555-0001, 29.8.2003
Kuva: https://u.osu.edu/engr2367nuclearpower/davis-besse/