KyLÄ-Innovation Platform

Bilhanan Silverajan

ville.haapakangas@tuni.fi jari.seppala@tuni.fi bilhanan.silverajan@tuni.fi

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

KyLÄ Programme: Cyberlabs for Smart Industry

The main goal of the KyLÄ project is to create an innovation and development platform in Pirkanmaa that is suitable for the needs of developing the cyber security of companies working in smart industry.

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

Research Platform and Labs

In TAU:

- Automation Cyberlab
- Computing Cyberlab
- Electrical Engineering Cyberlab
- Medical Technologies Cyberlab

In TAMK:

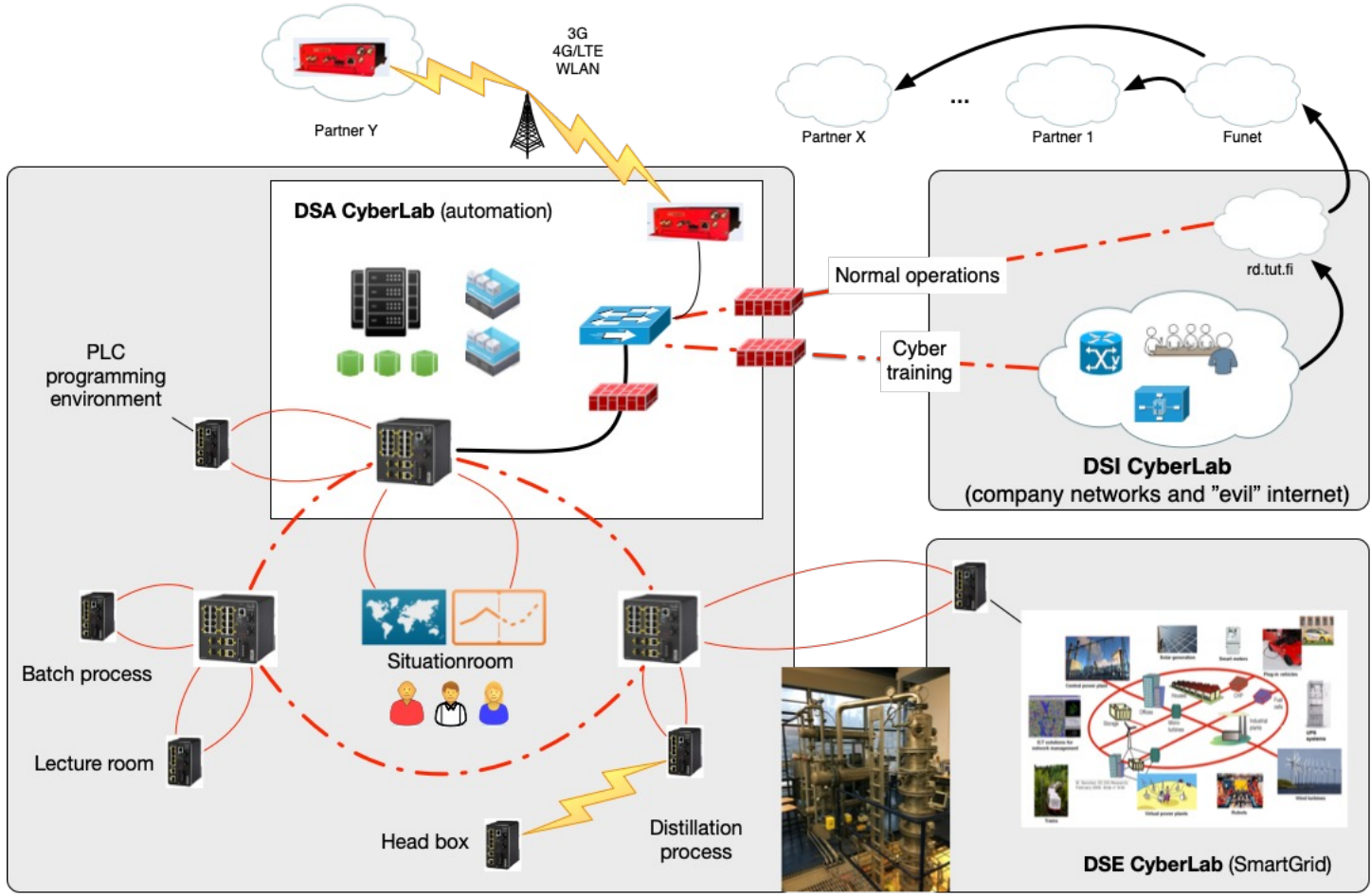
- ICT Lab
- CyberLab
- Process Automation Lab
- Machine Automation Lab
- Field Lab

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle
Tampereen yliopisto
Tampereen ammattikorkeakoulu
PIRKANMAA
Vipuvoimaa EU:lta 2014–2020
Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

Automation Cyberlab

Consists of industrial automation and control systems running the critical infrastructure.

It is built keeping in mind the long lifecycle and the challenges it will create.



KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

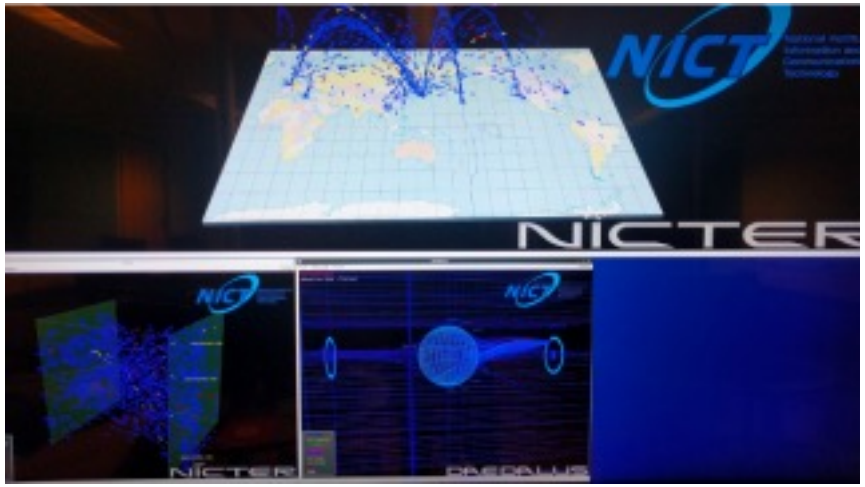
Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

Computing Cyberlab

Consists of network, secure communication and computing infrastructure.

This is used for teaching as well as for research with small and large enterprises as well as international research partners.



KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

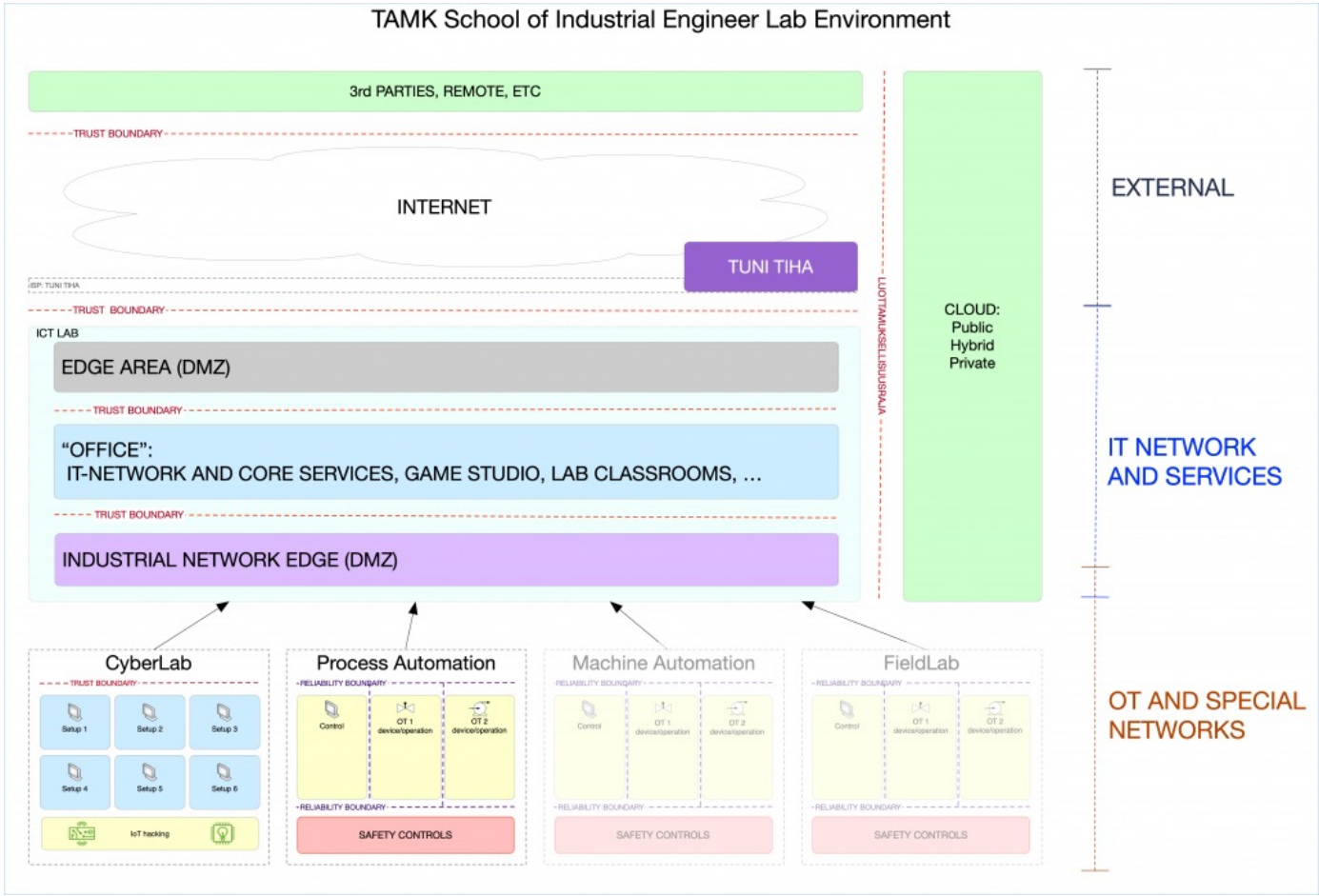
Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

TAMK ICT Lab

Research and studying facility that has been created to model a network and services of a large company.

Network offers connection to other lab environments (e.g. CyberLab, Machine Automation Lab, Process Automation Lab and Game Studio)

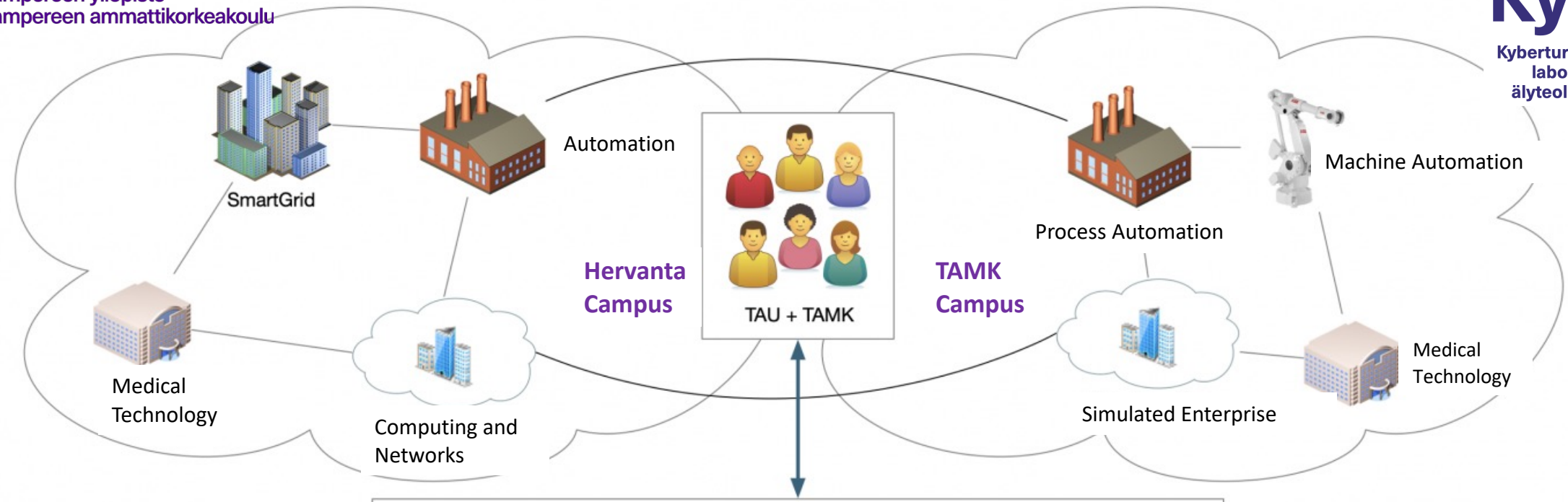


KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle
Tampereen yliopisto
Tampereen ammattikorkeakoulu
PIRKANMAA
Vipuvoimaa EU:lta 2014–2020
Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

KyLÄ - innovaatioalusta

Tampereen yliopisto
Tampereen ammattikorkeakoulu

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle



Contact Persons
Practices
Processes

Personnel
Organisations
Companies
Pirkanmaa Smart Industry Stakeholders

Expectations
Trust
Reliability

A technical "test bed" that offers companies the opportunity to (1) build and develop services, (2) create new concepts, (3) test future products and (4) develop expertise without the need to invest in their own expensive technical environments

PIRKANMAA

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

USE CASE: Deploying a security system

ROLES:	Industrial enterprise	Security company	TAU+TAMK Cyberlabs
What is desired:	test the establishment of remote management connections to production systems with a specific technical solution	provides an opportunity to test and test the system in the most authentic environment possible	produce new knowledge and practical, close research and learning opportunities for companies and students
Why:	Obtain information on the functionality and usability of the system before it is put into operation in production	In order for the customer to see the benefits of the system and gain user experience for it, they receive information about the use of the system	to ensure that researchers and students have up-to-date skills that meet the needs of the business world
Description:	The company wants to test a possible system in an authentic-like environment before acquiring it and incorporating it into its production environment	The company offers its potential customers a testing opportunity in an authentic operating environment	Allows the system to be used in a real network that mimics the operating environment of an industrial enterprise .
What do you get:	- The opportunity to test the product in an authentic environment - an unbiased view of the implementation, operation of the product, etc. - possibly the work/project/internship of a student who is familiar with the product for the role	- visibility of the product and feedback on its operation - Researchers, Students and teachers familiar with the product - the opportunity to present the product more widely to other companies - possibly the work/project/internship of a student who is familiar with the product for the role	- the opportunity to get acquainted with and use modern systems - an opportunity to study the functionality of the systems - exchange of information with both customer companies and supplier companies
What is the commitment:	- collaborative project	- Delivering the system for campus lab use	- Create and maintain a lab environment

USE CASE: Security testing of software and hardware

ROLES:	Business	Testers	TAU+TAMK Cyberlabs
What is desired:	Find out about the security of their products	Test systems to find security vulnerabilities	enables new learning of information security through hacking
Why:	Develop better products and find security vulnerabilities	to make systems better	to inform about security vulnerabilities
Description:	The company delivers its system (which can be hardware or software) to KyLÄ and is involved in its implementation. The company determines the terms of the testing and the outputs they want from the testers.	The tester (researcher, student, company's own employee) gets the opportunity to test the system in a controlled environment tailored for testing.	Enables the deployment of the system in the test environment and provides the required "background services" such as private cloud, AD, DNS, DHCP.
What you get:	- Test results	- the ability to test systems that are not frequently testable - a reward for observations made	- Room - students have the opportunity to participate in security testing
What is the commitment:	- Bring products for testing - pay predetermined fees	- ethical conduct - reporting results to the Product Owner	- creating and facilitating the event - Manage media coverage - facilities, network connections, etc. organize resources

Information reliability is not created by accident

- Reliable data enables reliable information
- Reliable data is produced by information technology
- Reliable information technology is by designing the environment so that the information is as reliable as possible
  - We are talking about integrity - the immutability of information/data during transfer and storage (and information is not always compromised by information security problems, a normal device failure or a wrongly connected cable can cause changes to the information)
  - We are talking about confidentiality - information/data can only be accessed by those who have the right to it (not stolen and published by criminals, for example)
  - We are talking about availability - information/data is available, available when it is needed (and not, for example, encrypted by ransomware, lost with a broken device or not in use when someone connected one of its cables to the wrong place and the computer stopped working)
- By transferring data for data processing using a reliable data transfer procedure
  - This does not always mean encryption with some complex system, but risk assessment and decisions regarding cost efficiency should not be forgotten
    - Eg a €10,000 firewall should not be installed to protect information worth 1 c.

Moving from unknown to known environments

- Get to know the environment, understand what has happened historically
- At the same time, the device list is recorded
  - Devices connected to the network are physically checked from the device/computer (device, communication technology, object/objects)
  - Computers with a universal operating system (Windows, someone else: what, operating system version, responsibility for maintenance including programs and operating system and configuration, licenses)
  - Let's think about what will happen if the device breaks down (criticality assessment, e.g. does the entire production stop and how long can the situation be tolerated)
- Let's draw a data flow diagram at the same time
  - Which device/computer talks to which device/computer, using which technology, technical details, e.g. address and port)
- Combining the above with the level model according to the standard (IEC-62443)
  - Which functional box does the device/computer belong to
- Let's consider a reasonable solution that can be used to transfer data to the cloud and back from the cloud.
  - Risks, need for preparation (e.g. does a communication outage completely prevent the use of the device)
- At the same time, we take notes of other possible issues
  - For example, that our last expert just retired, his phone number is 0401234567.

ISA99/IEC-62443 (värit 62443:n mukaiset)

Oman tuotantannon kokonaisuuksia ja automaatiota, ei vielä tietoturvaa

- **Taso 5** — Kolmannet osapuolet & Internet
- **Taso 4** — Yritysjärjestelmät
- **Taso 3** — Järjestelmän hallinta, ohjelmointi sekä integraatiot
- **Taso 2** — Tilan havainnointi, ylemmän tason säädöt ja paikallinen näyttö
- **Taso 1** — Paikalliset säädöt ja turvallisuus
- **Taso 0** — Laitteet

		Sijainti		
Kartoitus-ID	Tuotteen nimi/mallinro	Rakennus	Kerros	Huone

Toiminnalliset Kokonaisuudet

”Loogiset laatikot”

Mitä meillä on?

Oikeasti! Tarkastetusti

Tietoturvavyöhyke: 3-OSAPUOLI — Kolmannen osapuolen palvelut ja asiakkaat

LUOTTAMUKSELLISUUSRAJA

Internet

LUOTTAMUKSELLISUUSRAJA

Tietoturvavyöhyke: YRITYS-DMZ — Tyypillisesti ulkoistettu pk-yrityksillä -> ostamisen osaamista (ymmärrys, riskit) ja sopimuksia (vaatimuksia)

LUOTTAMUKSELLISUUSRAJA

Tietoturvavyöhyke: TOIMISTO — Osa itsellä, osa palveluina hankittua -> osaamista, sopimuksia

LUOTTAMUKSELLISUUSRAJA

Tietoturvavyöhyke: I(A)CS DMZ — Lisäturvaa tuova kerros -> hidastaa merkittävästi haittaohjelmien leviämistä ja kohdennettuja operaatioita

LUOTETTAVUUSRAJA

Tietoturvavyöhyke: Tilan valvonta, korkeamman tason säädöt ja paikalliset näytöt

Tärkein suojattava kohde tuotannon jatkuvuuden ja tiedon kannalta.

Valvomo 1

Valvomo 2

Turvallisuus ja suojaus

Tuotantoalueen 1 laite/oiminnallisuus

Tuotantoalueen 1 laite/oiminnallisuus

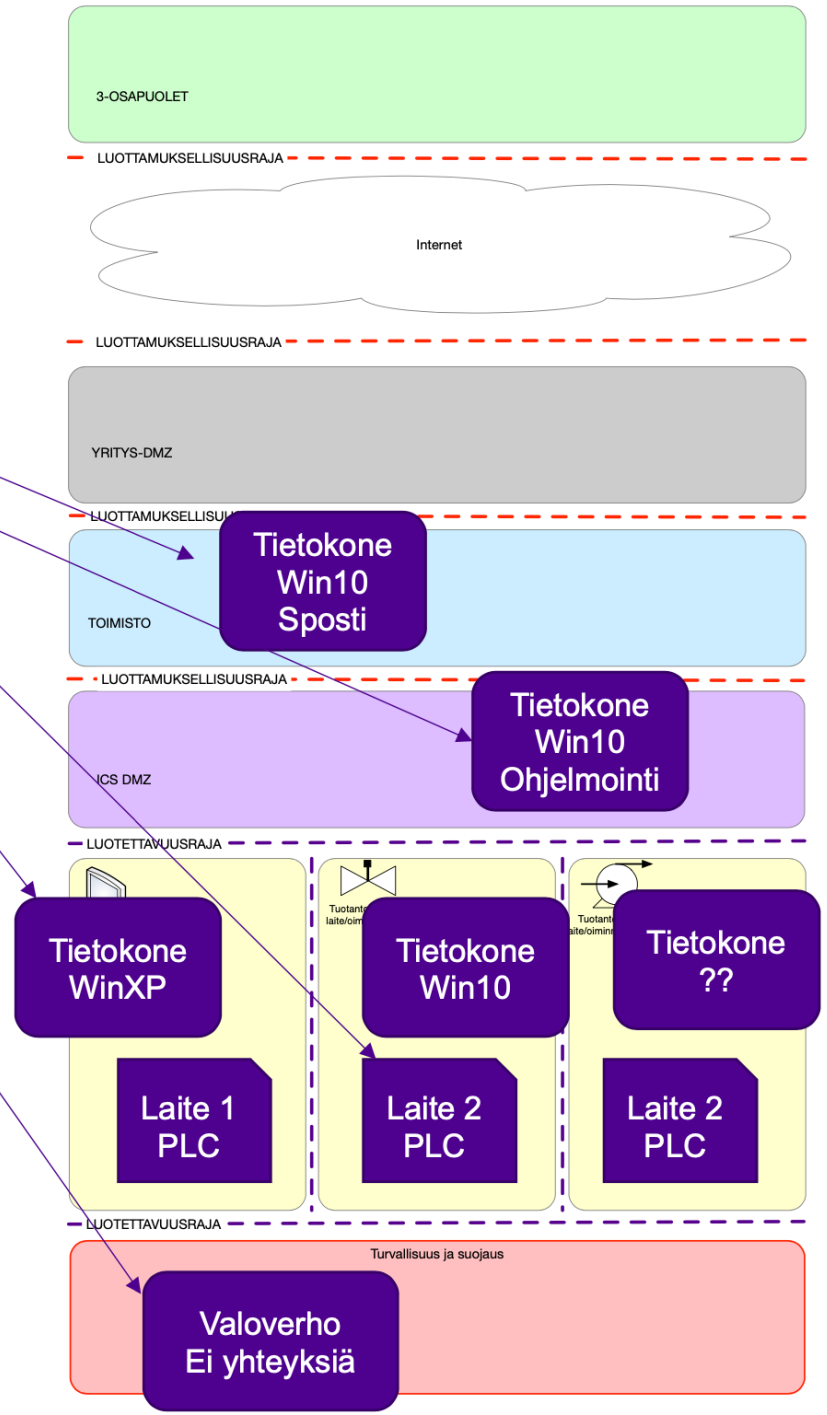
Tuotantoalueen 2 laite/oiminnallisuus

Tuotantoalueen 2 laite/oiminnallisuus

(c) Jari Seppälä, jari.seppala@tuni.fi

Tampereen yliopisto
Tampereen ammattikorkeakoulu

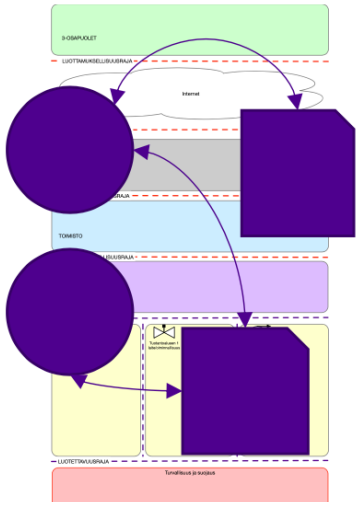
		Sijainti		
Kartoitus-ID	Tuotteen nimi/mallinro	Rakennus	Kerros	Huone



Place devices in suitable functional units (boxes)

Draw a picture of which device talks to which and what information is transferred (i.e. data flows)

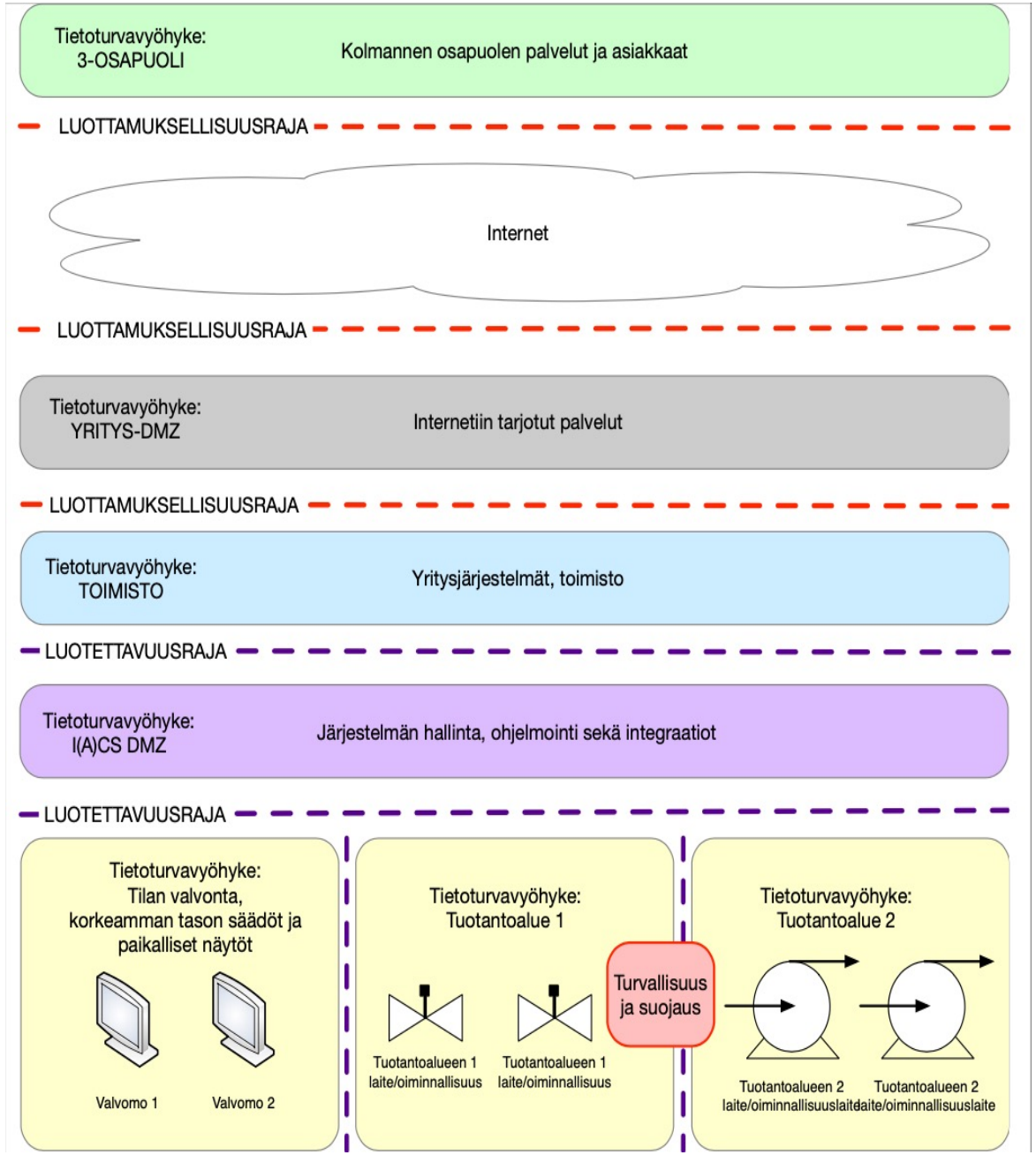
+

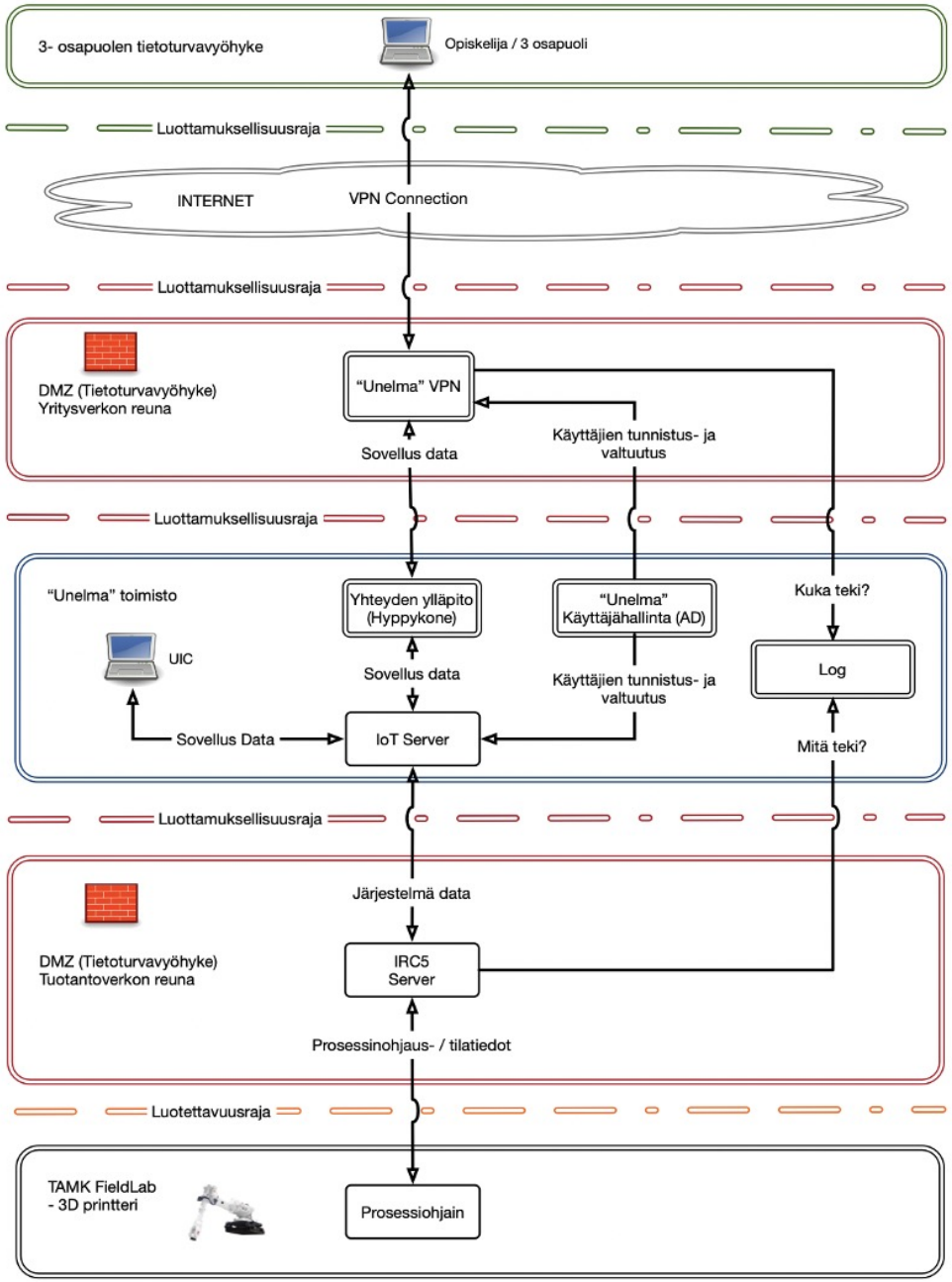


At the same time, an understanding of current production in an IT sense is created through discussions and a list of CRITICAL components for which it would be good to have a backup device

Euroopan unioni
Euroopan aluekehitysrahasto
Vipuvoimaa EU:lta 2014–2020
PIRKANMAA

(c) Jari Seppälä, jari.seppala@tuni.fi


Tietoturvavyöhyke:
3-OSAPUOLI
Kolmannen osapuolen palvelut ja asiakkaat
LUOTTAMUKSELLISUUSRAJA
Internet
LUOTTAMUKSELLISUUSRAJA
Tietoturvavyöhyke:
YRITYS-DMZ
Internetiin tarjotut palvelut
LUOTTAMUKSELLISUUSRAJA
Tietoturvavyöhyke:
TOIMISTO
Yritysjärjestelmät, toimisto
LUOTETTAVUUSRAJA
Tietoturvavyöhyke:
I(A)CS DMZ
Järjestelmän hallinta, ohjelmointi sekä integraatiot
LUOTETTAVUUSRAJA
Tietoturvavyöhyke:
Tilan valvonta,
korkeamman tason säädöt ja
paikalliset näytöt
Valvomo 1
Valvomo 2
Tietoturvavyöhyke:
Tuotantoalue 1
Tuotantoalueen 1
laite/oiminnallisuus
Tuotantoalueen 1
laite/oiminnallisuus
Turvallisuus
ja suojaus
Tietoturvavyöhyke:
Tuotantoalue 2
Tuotantoalueen 2
laite/oiminnallisuuslaite
Tuotantoalueen 2
laite/oiminnallisuuslaite


3- osapuolen tietoturvavyöhyke
Opiskelija / 3 osapuoli
Luottamuksellisuusraja
INTERNET
VPN Connection
Luottamuksellisuusraja
DMZ (Tietoturvavyöhyke)
Yritysverkon reuna
"Unelma" VPN
Sovellus data
Käyttäjien tunnistus- ja
valtuutus
Luottamuksellisuusraja
"Unelma" toimisto
UIC
Yhteyden ylläpito
(Hyppykone)
Sovellus data
"Unelma"
Käyttäjähallinta (AD)
Käyttäjien tunnistus- ja
valtuutus
Kuka teki?
Log
Sovellus Data
IoT Server
Mitä teki?
Luottamuksellisuusraja
Järjestelmä data
DMZ (Tietoturvavyöhyke)
Tuotantoverkon reuna
IRC5
Server
Prosessinohjaus- / tilatiedot
Luotettavuusraja
TAMK FieldLab
- 3D printteri
Prosessiohjain

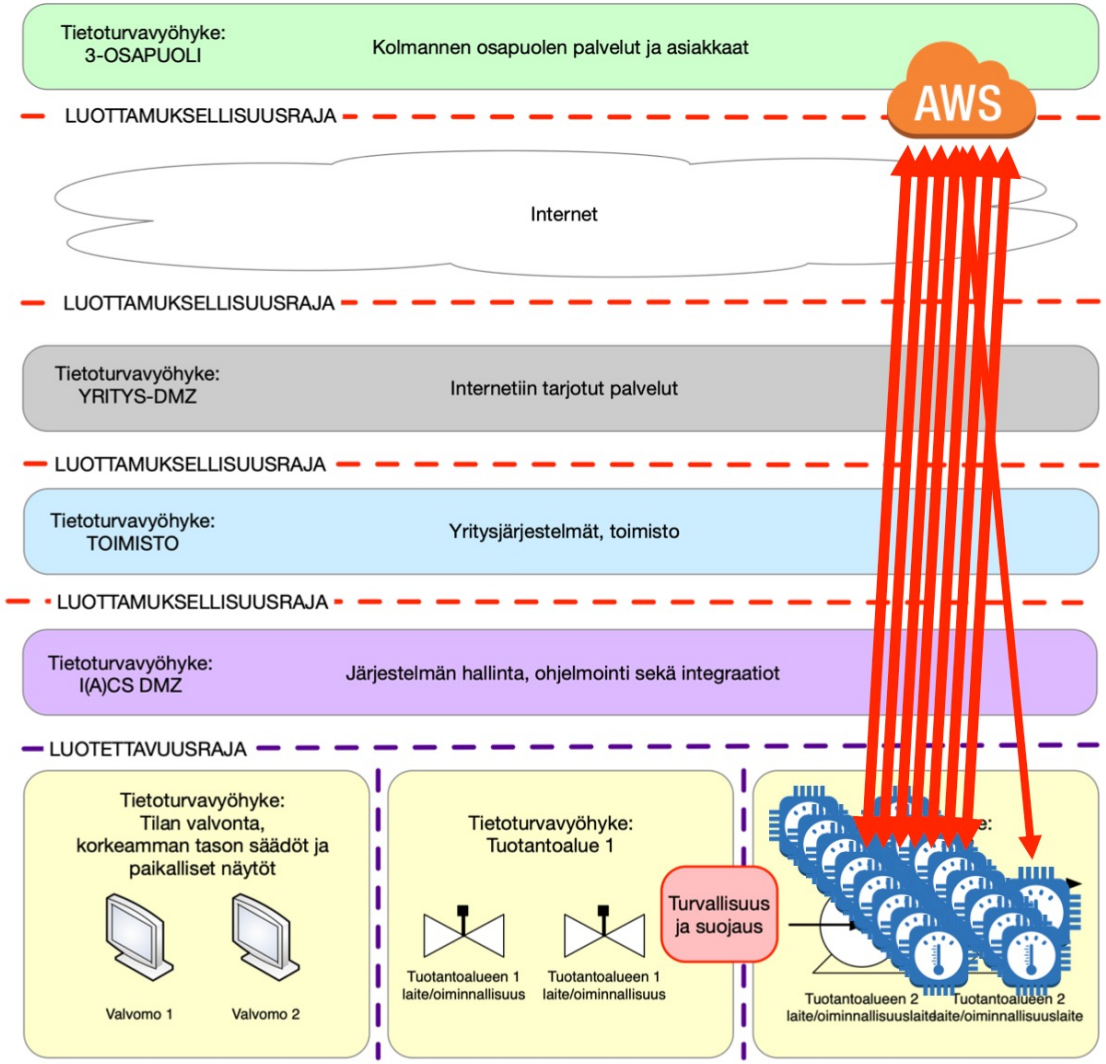
© Jari Seppälä

Risks to operational environments coming from 3rd party requirements

The vendor wants to sell an IoT solution where "data is analyzed in the cloud”

- Let's draw a logical model
- Let's think about the risks

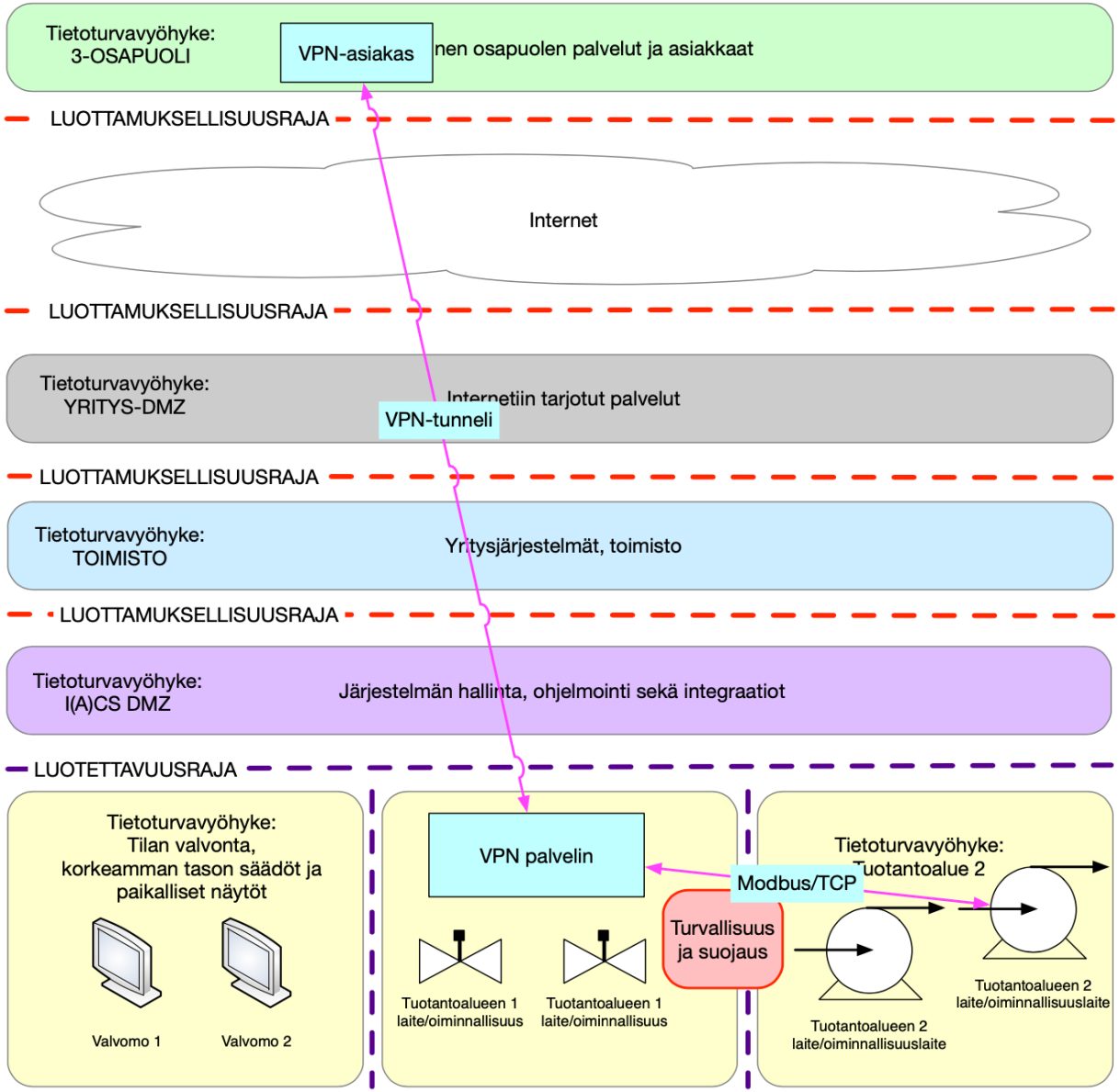
If there are several independent suppliers, how many holes do you want to “drill” into your own environment?



A common data pattern

Investigate the vendor solution on top of the model

- Check the description and documentation
- Monitor the implementation and correlate for correctness
- Plan your own data transfer, e.g. to cloud services
- Transferring information does not mean that communication is free and direct.
- Is a VPN used or required by the solution?
    - the task is to hide the connection from outsiders, so the pipe cannot be seen
    - Is only as reliable as endpoints
    - Who controls and who is responsible for the VPN client's data security?



(c) Jari Seppälä, jari.seppala@tuni.fi

Tampereen yliopisto
Tampereen ammattikorkeakoulu

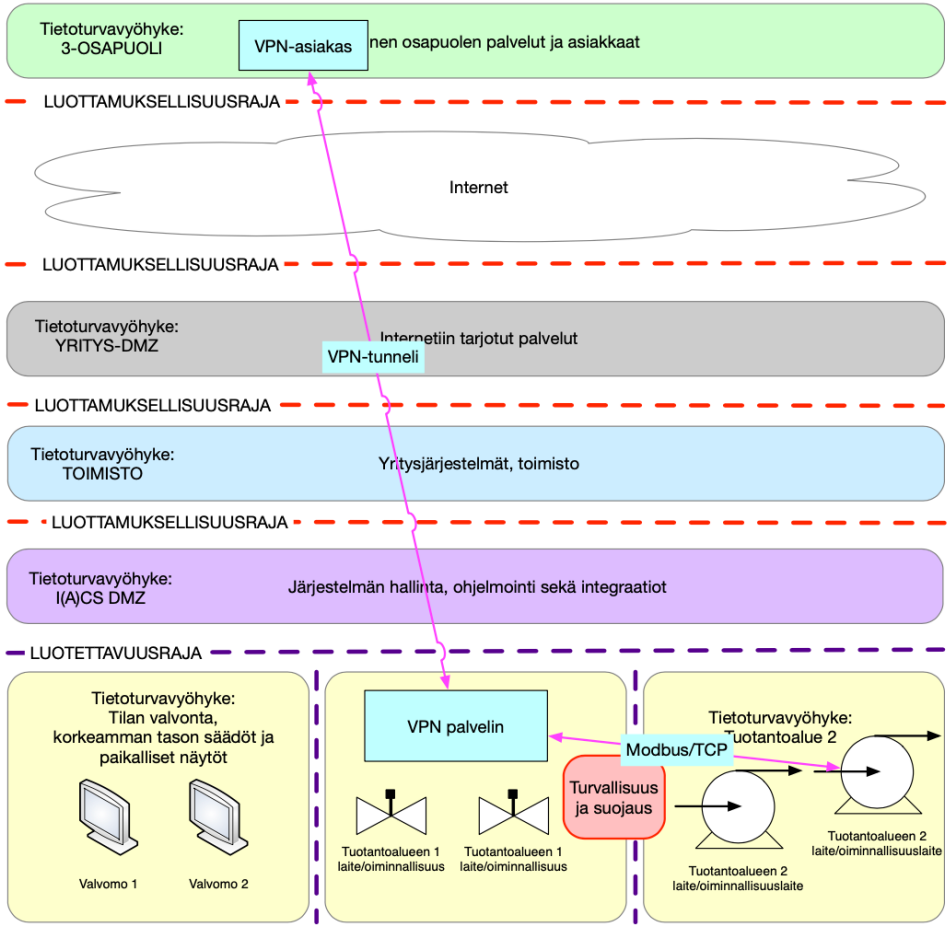
Euroopan unioni
Euroopan aluekehitysrahasto

Vipuvoimaa EU:lta 2014–2020

PIRKANMAA

Simple, vendor recommended solution

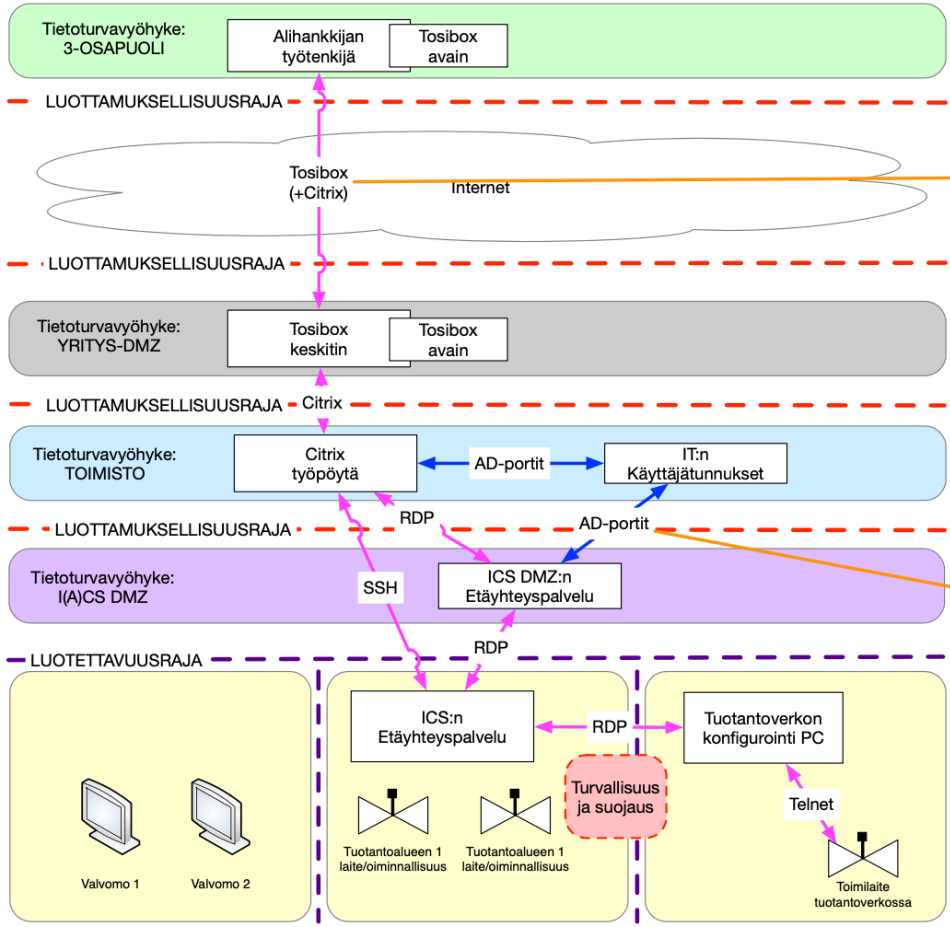
But it bypasses all security and trust zones and can cause uncontrollable data leakage and privacy problems!



A more complex way that is under the control of the owner

Enables data reliability, thoughtful data transfer and reduces the risk of uncontrolled data leakage

(Note! Get a partner to implement, you don't have to and shouldn't do everything and manage it yourself)



Tukevassa dokumentaatiossa jos iso lista, muuten kuvassa

Tosibox dokumentaatio

Alihankkijakäytäntö

Protocol and Port	AD and AD DS Usage	Type of traffic
TCP and UDP 389	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP
TCP 636	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP SSL
TCP 3268	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC
TCP 3269	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC SSL
TCP and UDP 88	User and Computer Authentication, Forest Level Trusts	Kerberos
TCP and UDP 53	User and Computer Authentication, Name Resolution, Trusts	DNS

(c) Jari Seppälä, jari.seppala@tuni.fi

Partners involved now

Company participation needed – We aim to meet those needs!

KyLÄ cyberlabs can be flexibly used with different configurations:

- Radiator Software Oy
  - Testing, development and analysis of PKI, AAA and RADIUS-based systems
- Mideye Oy
  - Testing and integration and interoperability of MFA and authentication for OT/Factory networks

In discussions:

- WatchMyDC
  - Using Clouds and VMs to deploy Collector service for data and security automation

Going Forward

Currently:

- Continual improvements to technical environments
- Envisioning Industrial Use cases
- Tests and developments with companies

From 2023:

- Cyberthreat Intelligence and Situational Awareness: Development, Data Collection and Testing

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle
Tampereen yliopisto
Tampereen ammattikorkeakoulu
PIRKANMAA
Vipuvoimaa EU:lta 2014–2020
Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

For more information

Ville Haapakangas:

ville.haapakangas@tuni.fi, 050 5287013

Kylä-hanke ja innovaatioalusta:

https://projects.tuni.fi/kyla/

Tampereen korkeakouluyhteisön kyberturvallisuuden toimijat ja labrat:

https://research.tuni.fi/dependablesystems/

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

Thank you!

KyLÄ
Kyberturvallisuuden laboratoriot älyteollisuudelle

Tampereen yliopisto
Tampereen ammattikorkeakoulu

PIRKANMAA

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto