OPC and MES DAY

15 October 2013, Tampere

Improving manufacturing IT security with OPC UA

Pasi Ahonen, Senior Scientist,
COREQ-ACT project manager,
VTT Technical Research Centre of Finland

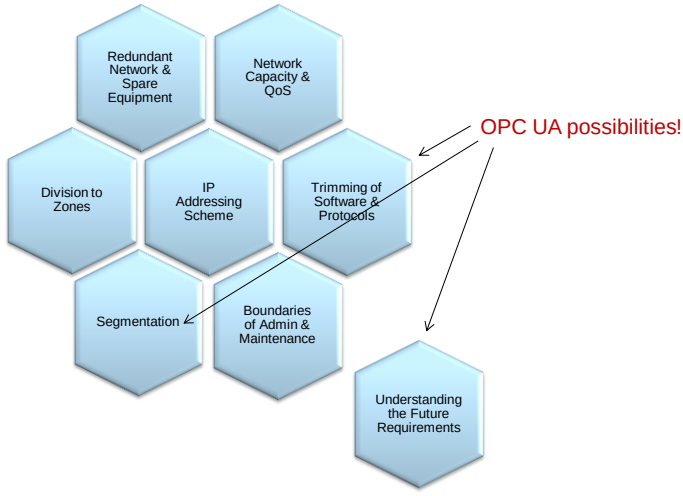
Agenda

1. *What is manufacturing IT Security?*
2. *Improving manufacturing IT security…*
   - ✓ *2.A) Using OPC UA protocols*
   - ✓ *2.B) OPC UA security*
3. *Finally, few words about some national projects*
   - ✓ *Done: TEO-TT, COREQ-VE, COREQ-ACT*
   - ✓ *Coming 2014: KYBER-TEO*
   - ✓ *National Emergency Supply Agency (www.nesa.fi) as main project owner*

Adapting COREQ-VE & COREQ-ACT results

1. What is manufacturing IT Security?

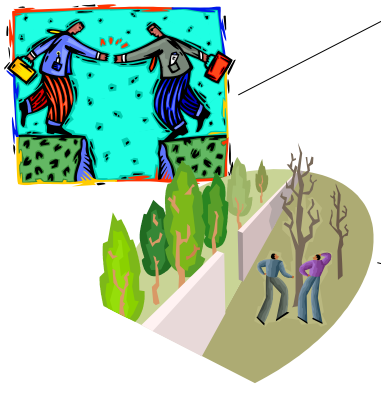
At least the following network view, but that is not all of it!



1. What is manufacturing IT Security?

Division to Zones & Segmentation

Division to Zones & Segmentation



ZONING (The Zones), e.g.:

- ❑ **CORPORATE NETWORK**
- ❑ **PLANT NETWORK**
- ❑ **VISITOR NETWORK: WiFi, using IEEE 802.1X, RADIUS…**
- ❑ **DMZ: TERMINAL SERVICES, PROXIES & DMZ-SERVICES, OPC UA clients/servers**
- ❑ **SUPERVISORY: HMI, SERVERS…**
- ❑ **R&D: ENGINEERING STATIONS, TEST NETWORKS...**
- ❑ **AUTOMATION NETWORKS: PROFIBUS, PLC-COMM, I/O…**
- ❑ **SAFETY INSTRUMENTED SYSTEMS**

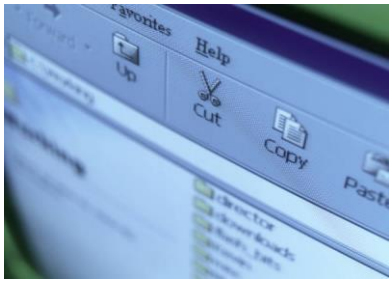
PHYSICAL SEGMENTATION:

- ❑ **SEPARATE SWITCHES:**
  - ✓ **Plant network and automation network in separated switches**
- ❑ **CABLES: Network cables clearly differentiated and marked, E.g.:**
  - ✓ **Separate production lines**
  - ✓ **Separate delivery segments, etc.**
    - o **Managing also the reserve**

1. What is manufacturing IT Security?

Trimming of Software & Protocols

Trimming of Software & Protocols



- **GOOD CONTROL: Limited applications, OS and other software in each Zone/Segment**
  - ✓ E.g. Vendor maintained subnetwork
  - ✓ Only automation mgmt approved software
  - ✓ Similar protocol stack in each device of a subnet
- **SIMPLE RULES: Simplify FW rules using limited apps and protocols**
  - ✓ Deny everything by default in FWs
  - ✓ In/Out: OPC UA data simplify FW traverse!
    - ❖ Prefer the traverse of OPC UA applications!
  - ✓ Ext.connections: OPC UA inside VPN tunnel
    - ❖ Allow authorized VPN tunnels to dedicated DMZ area proxy server!
  - ✓ OPC UA based security (when feasible).

1. What is manufacturing IT Security?

Boundaries of Admin & Maintenance

Boundaries of Admin & Maintenance

NETWORK admin / maintenance RESPONSIBLES must be defined clearly:

- **ZONE: Subnetwork/ Segment: responsibles!**
  - ✓ Independent zone/subnet operation
  - ✓ Cabling standards, colors and markings in zone
  - ✓ Reserve store: Standard cables & connectors
- **WORKSTATIONS: Maintenance of general purpose workstations for automation:**
  - ✓ E.g. IT department maintenance according to automation determined requirements and guidelines
  - ✓ OPC UA client/server workstation maintenance
  - ✓ OPC UA Gateway services
- **WORK PERMIT: Management permission for connecting maintenance device to the network:**
  - ✓ Production mgmt,
  - ✓ Automation mgmt,
  - ✓ NOTE: Require OPC experience when maintaining OPC UA systems!

2. Improving manufacturing IT security…

2.A) Using OPC UA protocols

- ✓ **opc.tcp://Server** = OPC UA binary protocol**,** and
- ✓ **http://Server** = OPC UA Web Service.

Important to know:
WS-Security Performance

http://en.wikipedia.org/wiki/WS-Security

WS-Security adds significant overhead to SOAP processing due to the increased size of the message on the wire, XML and cryptographic processing.

A benchmark in 2006 (*Francois Lascelles, Aaron Flint: WS Security Performance. Secure Conversation versus the X509 Profile*) resulted in:

Security Mechanism	**Messages/second**
WS-Security (X.509) XML Signature & Encryption	352
WS-SecureConversation XML Signature & Encryption	798
Transport Layer Security	2918

WS-SecureConversation = to establish security contexts for multiple SOAP message exchanges
Transport Layer Security = TLS/SSL

For OPC UA and other data communication…

Simplify the used ICS data services!

REASONING: Simplicity of the allowed data flows makes it much easier to detect malicious attacks & vulnerable configurations!

OBJECTIVE: Goal is to be able to define easily MANAGEABLE Access Control Lists (ACLs) in switches and firewalls.

MAIN ACTIONS: Simplify all of your ICS systems' data access services

- Limit the number of used protocols, services, ports, etc.
  - ✓ Simplify local ICS data access (e.g. OPC Wrapper/Proxy)
  - ✓ Simplify remote ICS data access (e.g. OPC UA, RDP, VNC, SSH)
- Limit the number of allowed communicating hosts/peers

ADVANTAGES:

- SIMPLIFIES the monitoring configuration, increases the EFFECTIVITY of security solutions
- Gives more ACCURATE security monitoring results (less false positivies/negatives)

For OPC UA and other data communication…

REQUIREMENTS:

REQ: Mandate only specific data PROTOCOLS via specified PORTS

- Enable only the essential data transfer needs
- Allow only few different protocols and ports (in specific direction)
  - **In Firewalls, e.g. OPC UA discovery and actual private ports**

REQ: Mandate only specific data SOURCE and DESTINATION pairs

- Enable only the **legitimate** communication peers
- Allow only from specific source address to specific destination
- Analyse multicast data separately and typically isolate industrial-Ethernet to dedicated segments

REQ: Reduce the APPLICATIONS that are allowed via remote connections

- Allow **only certain applications** with reduced access rights & permissions
  - E.g. implementation via OPC UA client/server etc., depending on your environment
- Prohibit all potentially dangerous remote operations
- Disable direct database queries, remote network scanning functionality, etc.
  - Allow these only for special controlled cases, where other options are not possible

For OPC UA and other data communication…

Select secure remote connection technology solution!

REQUIREMENTS:

REQ: Mandate a predefined ”company standard” VPN tunnelling solution for all allowed remote connections to your production

Alt. 1: IKE/IPSEC tunnel based VPN: Standardize IKE and IPsec policies for connectivity:

- Requires configured VPN client at remote computer
- IKE authentication: VPN authentication mode selection (”*Main Mode*” protects the identity of peers, “*Aggressive Mode*” doesn’t)
- IPsec: Select parameters defining the exact cryptography for ESP protocol tunnels

Alt. 2: SSL tunnel based VPN solution

- Typically requires at least a web browser at the remote user
- You must decide whether browser shall or shall not allow plug-ins’ and active content (which may also be security risks)
- Requires a feasible browser plug-in if you want to pre-assess (e.g. virusscan) throughout the remote computer before granting the remote access

NOTE: You might need to define one company standard solution for IKE/IPsec tunnels and another standard solution for SSL tunnels!

Practical example: Define your allowed services!

Next example shall demonstrate the data services definition that shall be allowed through remote access

- **All other data traffic should be regarded as errors, attacks or other anomalies!**
- **NOTE: Even inside your allowed flow there might be an advanced attack.**

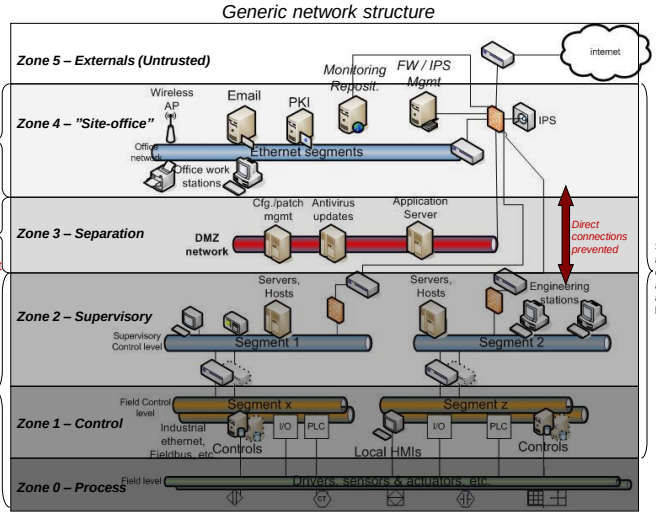
First thing, Secure Network Structuring

"Site" services:
- Firewall is the access point at site for receiving the remote connections
- IDS/IPS co-operating with firewall

Application server mediation:
- Protocol termination points
- No direct connections through!
- External OPC UA connection point

Each device has well defined:
- Comm. peers, protocols, ports, MAC addresses
- Input validation
- Interface capacity
- Configuration access ctrl.
- Controlled SW upgrades
- Emergency communication

Generic network structure



Securing the remote access!

Service Center

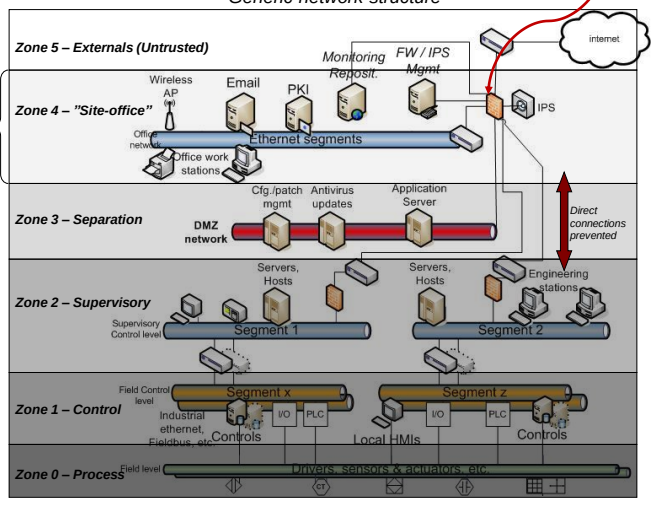
Practical example:
Define your allowed services!

Allow "a standard VPN tunnel" from CORPORATION to Site Firewall.

Allowed services (examples):
- **IKE**
- **ESP**
- **HTTPS**

Optional: Remote access only by request: Site firewall operator grants/deny online each remote access request. NOTE: Often this may not be practical due to lack of personnel.

Generic network structure

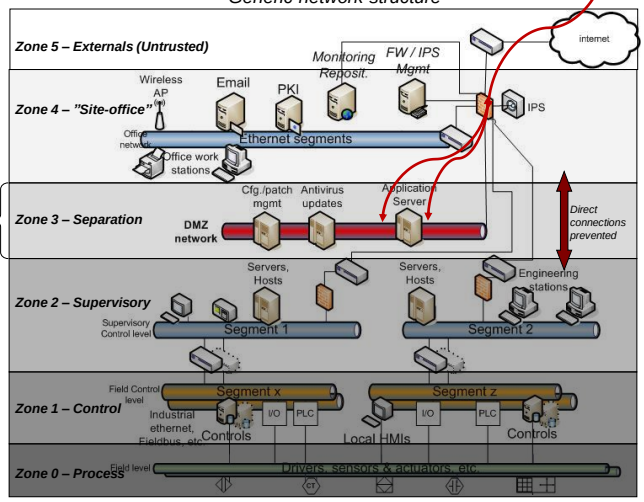


Securing the remote access!

Service Center

Practical example:
Define your allowed services!

Generic network structure



Within VPN tunnel, allow inbound connections from CORPORATION to a server at DMZ area.

Allowed services (examples):

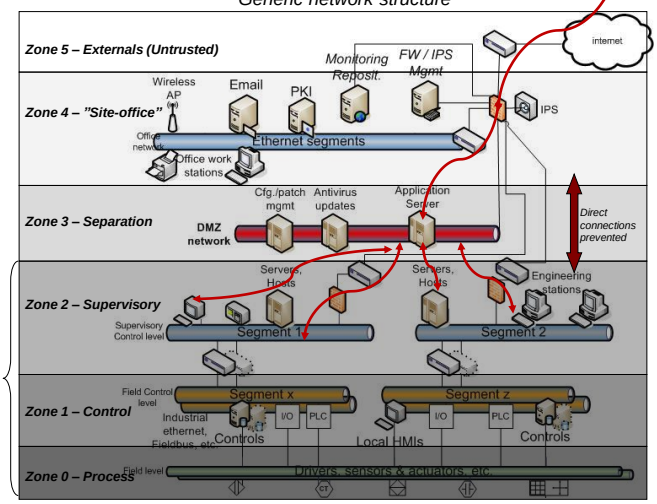
- **Application server supported OPC UA "binary protocol - opc.tcp://Server "**
- **RDP**
- **ICMP for ping?**

Securing the remote access!

Service Center

Practical example:
Define your allowed services!

Generic network structure



Allow certain services from a server at DMZ to certain hosts at control network.

Allowed services (examples):

- **RDP for operator remote desktop**
- **SSH for device configuration**
- **OPC UA for data gathering**
- **ICMP for ping**

2. Improving manufacturing IT security…
2.B) OPC UA security

only the very basics…

OPC UA security

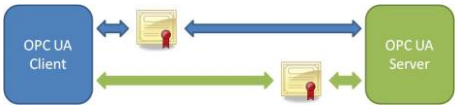
http://www.ni.com/white-paper/13843/en/

"In Classic OPC,
- developers must use Access Control lists stored in DCOM settings to configure the security settings for each component."

"In contrast, OPC UA
- uses standard web technologies as a security foundation including both authentication and encryption capabilities to protect data."

OPC UA security

http://www.ni.com/white-paper/13843/en/



- "OPC UA supports PKCS12 Public-Key Cryptography Standards to provide the X.509 private keys and certificate files that contain public keys."
- "To communicate between the server and client, the user can choose from three kinds of messaging modes: None, Sign, Sign and Encrypt."
- "Additionally, the user can enable one of the two security policies: Basic256 and Basic128Rsa15."

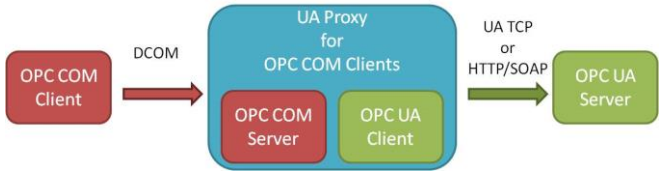
IT integration

http://www.ni.com/white-paper/13843/en/

- "OPC UA can communicate through any standard HTTP or UA TCP port."
- "OPC UA supports two protocols:
  - ✓ a binary protocol that employs minimal resources, allowing for easy enablement through a firewall; and
  - ✓ a Web Service protocol (SOAP) which uses standard HTTP/HTTPS ports."
- "Through this standardization, OPC UA can connect securely over a VPN and through firewalls to allow seamless, remote client-to-server connectivity."

UA Proxy

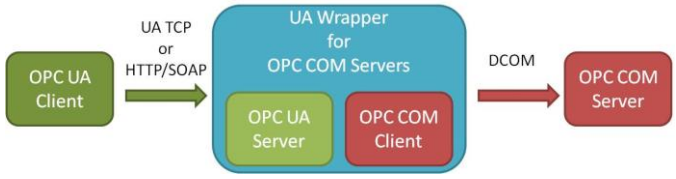
http://www.ni.com/white-paper/13843/en/



OPC UA protocol is not backwards compatible with Classic OPC data access (DA) models.

UA Wrapper

http://www.ni.com/white-paper/13843/en/



Example: Security requirements for Historian data collection

Number	Class	Objective	Security act	Scope G = Gen. M = O&M P = Project	Importance 1 = Minimum 2 = Option 3 = Advanced 4 = N/A (Out)	Requirement	Responsible V=Vendor P=Principal Other=?	Additional requirements	Implementation example
59	Historian data	Robust historian data collection	Standard historian data communication	P	2	Vendor system has capability to collect historian data using an open standard communication protocol	V+P		OPC UA with security, HTTPS
60	Historian data	Robust historian data collection	Secure historian data communication	P	2	Vendor shall provide a method for collecting historian data securely	V		Security capability in OPC UA, OPCXI, TLS/SSL

Ref: COREQ-ACT: "SECURITY REQUIREMENTS FOR INDUSTRIAL AUTOMATION VENDOR MANAGEMENT"

NOTE1: The classical OPC data is insecure. *It defines Microsoft COM/DCOM interface for data access (DA), historical data access (HDA), and alarms and events (A&E).*
NOTE2: *OPC Xi (OPC Express Interface) defines .NET interface functionality for OPC DA, HDA, A&E.*

Example: OPC UA Server Ports

The hardening of OPC-UA server

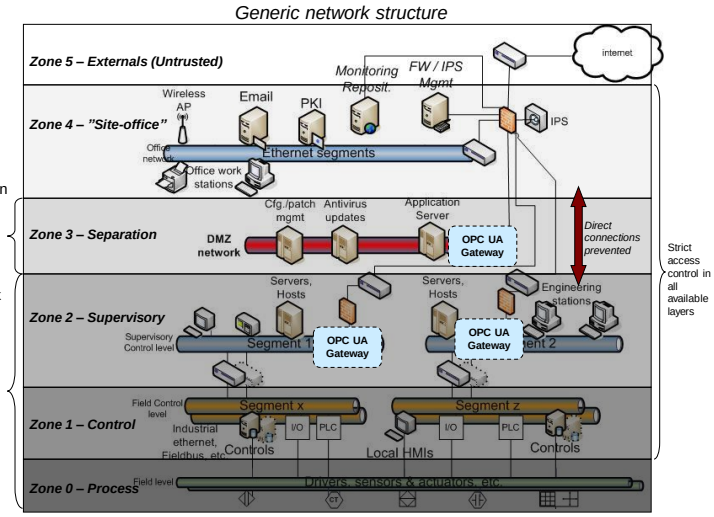
- Case-by-case hardening guide must be defined!
- OPC UA itself uses message based security
  - *Via* HTTP, UA TCP *port* or any other single *port*
- About ports:
  OPC UA server may serve many UA clients, each hosted on a different port
  - **4840**: *"OPC UA TCP Protocol for OPC UA":* to discover OPC UA services
  - **4843**: *"OPC UA TCP Protocol over TLS/SSL for OPC UA":* to securely discover OPC UA services
  - **Dynamic/Private ports**: 49152-65535: Session specific OPC UA service process

If you have Classical OPC…

Find your feasible options to isolate the insecure classical OPC data

- ✓ **OPC UA Gateway** enabling cooperation with OPC UA conversions
  - ➢ OPC DA ←→ OPC UA
  - ➢ OPC AE ←→ OPC UA, or
- ✓ Tunnel Classical OPC inside VPN (*not recommended above Zone 3*), or
- ✓ Reduce Classical OPC to local network

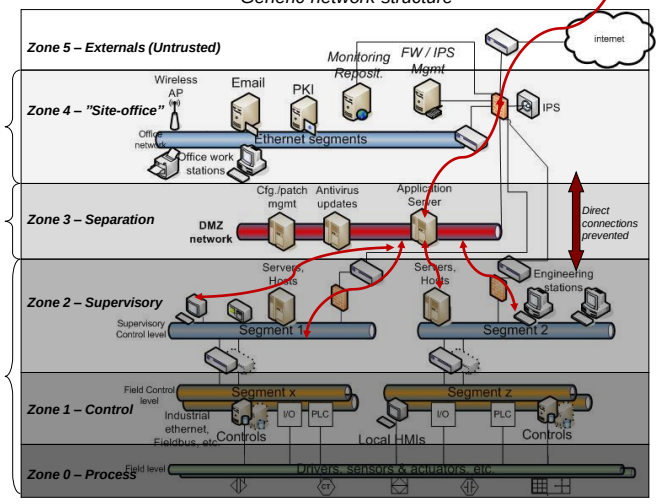
Generic network structure



IDS/IPS monitoring OPC UA & other

Service Center

Generic network structure



Keep your IDS/IPS automatically up-to-date against threats
Keep your rule setting simple
Automatically pick up the high risk events for closer analysis
Utilize filters that remove actions from some events
Filter out trusted IP addresses
Utilize summarization to decrease the volume of alerts

3. Finally, few words about some national projects

COREQ-ACT results are now available!

Tested concepts for implementing cyber security to industrial production

Project Goal: National Emergency Supply Agency owned and VTT led *"Active industrial cases for information security" (COREQ-ACT)* project created tested concepts for implementing cyber security requirements and practices to real-life industrial production environments. The results were based on real company cases, wide networking & reviews.

To whom: Personnel of any company or organization who may affect to the planning, procuring, design, implementation, testing, operating, or maintaining of an automated industrial production or system.

Results:

1. Cyber Security rules in the Factory (model example)
2. Security requirement base for industrial automation vendor management
3. Data security guidelines for procuring automation systems
4. Cyber security in production maintenance (training material)
5. Deploying the automation network cyber security
6. Remote access models to automation systems
7. Cyber security monitoring of remote service connections in practice
8. Application whitelisting product evaluations

Detail Information:
Pasi Ahonen, Senior scientist, VTT
phone: 020 722 2307
pasi.ahonen@vtt.fi

www.vtt.fi

Concerns: All groups:
- Production & Maintenance personnel
- Project personnel, vendors, service vendors
- External maintenance (device suppliers, mechanics, …)
- Other suppliers, truckers, cleaners
- External visitors

Concerns:
- All employees who plan, execute or participate to the procurement of automation systems, SW or devices
- Automation system vendors

Concerns: Production & Maintenance personnel

Concerns: All groups

Concerns: Vendors, own technical personnel

Concerns: System administration, service vendors

Concerns: Vendors, own technical personnel, procurement, etc.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

cert-fi Viestintävirasto

A new national project is under preparation: KYBER-TEO ”Improving cyber security for industry”

Developing and testing <u>SERVICES</u> in the participating companies to ensure the cyber security and continuity of Finnish industrial production

WP 1: Cyber security practices and mappings (2014-2015)
WP 2: Deploying the cyber security to industrial production (2014-2016)
WP 3: Cyber security monitoring services for automation networks (2014-2016)

Project preparation process:
- DISCUSSIONS: First, VTT starts the case discussions with interested companies
- PLANNING MEETING: A multilateral preparation meeting at ~November 2013
- TENDERS: Tenders to companies: ~December 2013
- KICK OFF: 1st steering group meeting at January 2014

GOAL: To disseminate results and experiences between companies.

Detail Information & participation to project KYBER-TEO, please contact:
Pasi Ahonen, Senior scientist, VTT
phone: 020 722 2307
pasi.ahonen@vtt.fi