Tieturvapalvelut osana automaation palveluliiketoimintaa

Automaation tietoturvallisuuden teemapäivä
16.10.2013

Teemu Kiviniemi
Tuotepäällikkö
Metso Automation

Esityksen agenda

- Metso Automation
- Metso DNA automaatiojärjestelmän arkkitehtuuri
- Toimisto- ja automaatioverkon erot
- Tietoturvan huomioiminen osana automaatiojärjestelmätoimitusta
- Tietoturvapalvelut osan laitoksen elinkaaripalveluja
- Tulevia haasteita automaation tietoturvan suhteen

Laaja automaation ja informaatioteknologian tarjonta

Liiketoiminta- ja palveluratkaisut

Automaatiojärjestelmät (prosessin, koneen ja käyttöjen ohjaus)

Edistynyt prosessinohjaus

Kunnon ja ajettavuuden valvonta

Tiedonhallinta

Radanvalvonta ja vianilmaisinjärjestelmät

Laadunvalvontajärjestelmät

Profilointilaitteet

Analysaattorit ja erityismittalaitteet

Älykkäät asennoittimet

Automaattiset on/off venttiilit

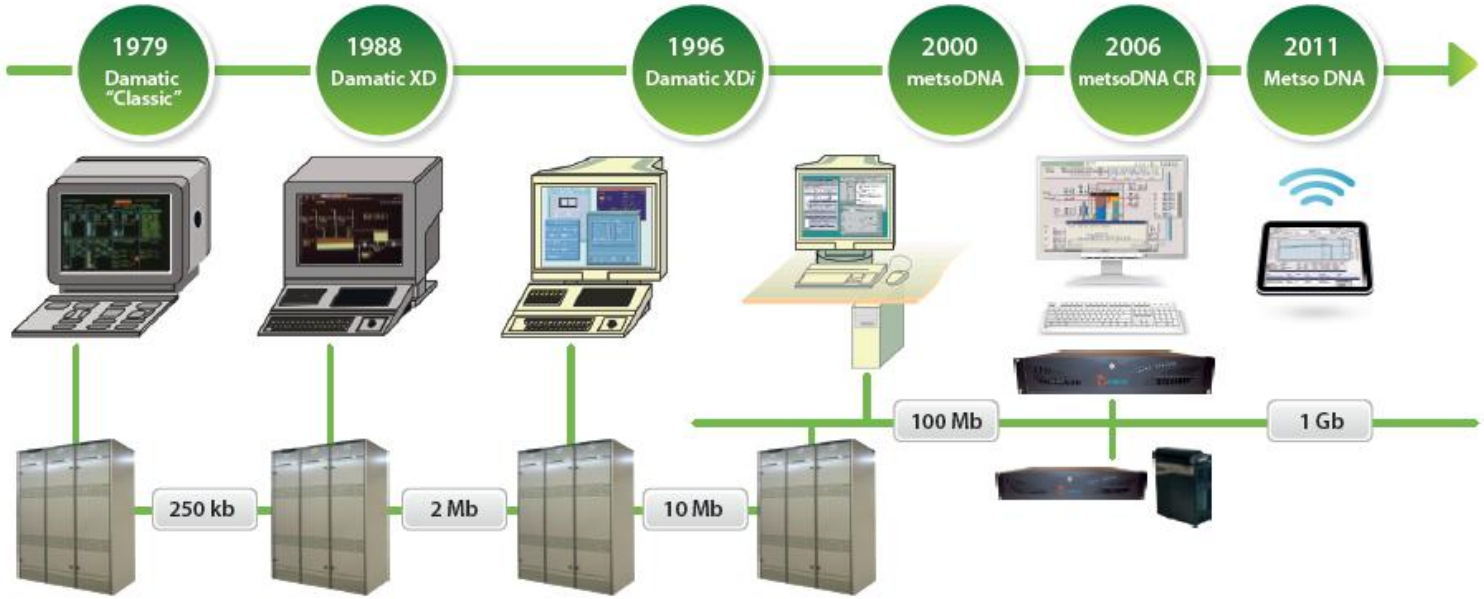
Säätöventtiilit

Hätäsulkuventtiilit

Metso DNA

Prosessiautomaatiojärjestelmä

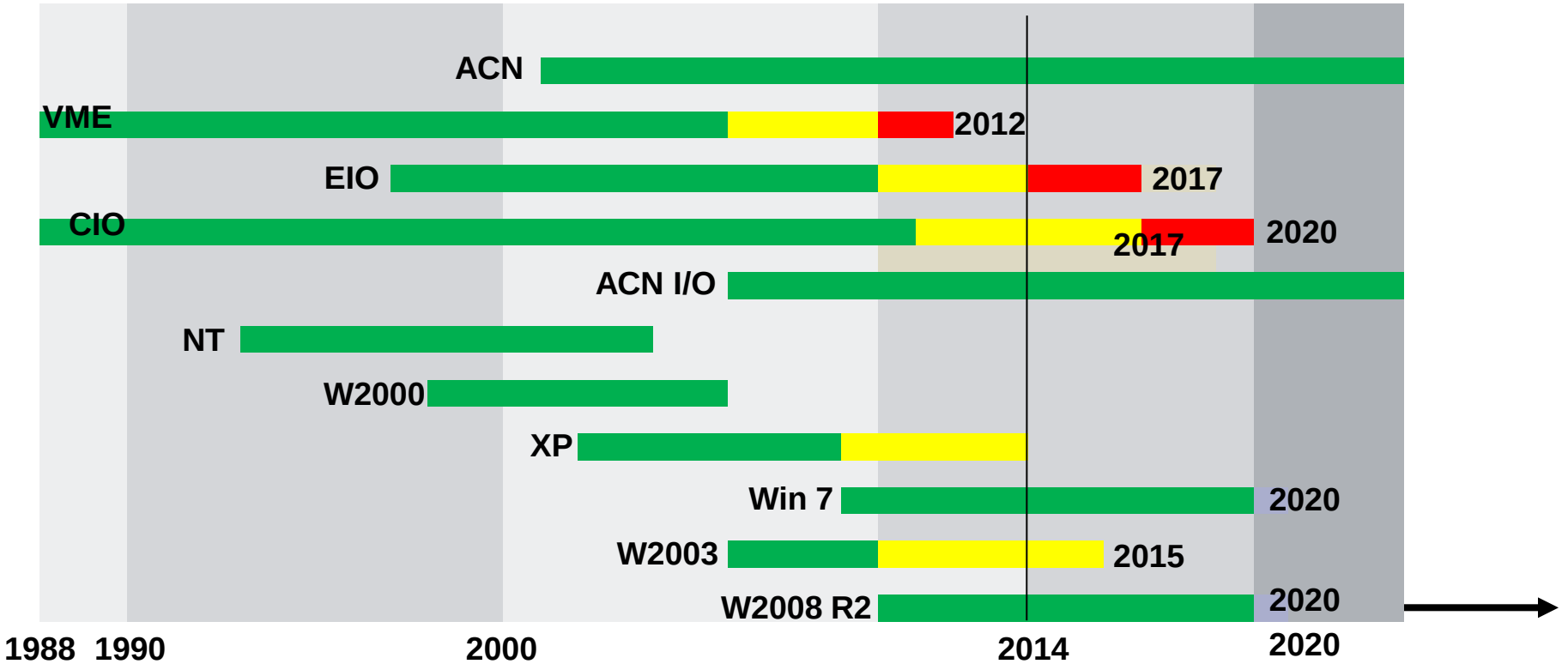
Upgradeability with innovative evolution



- Connectability
- Upgradeability
- Openness
- Same platform for all applications

- User friendly
- Flexible
- Reliable
- Long experience of developing control systems

Automation system technology over decades

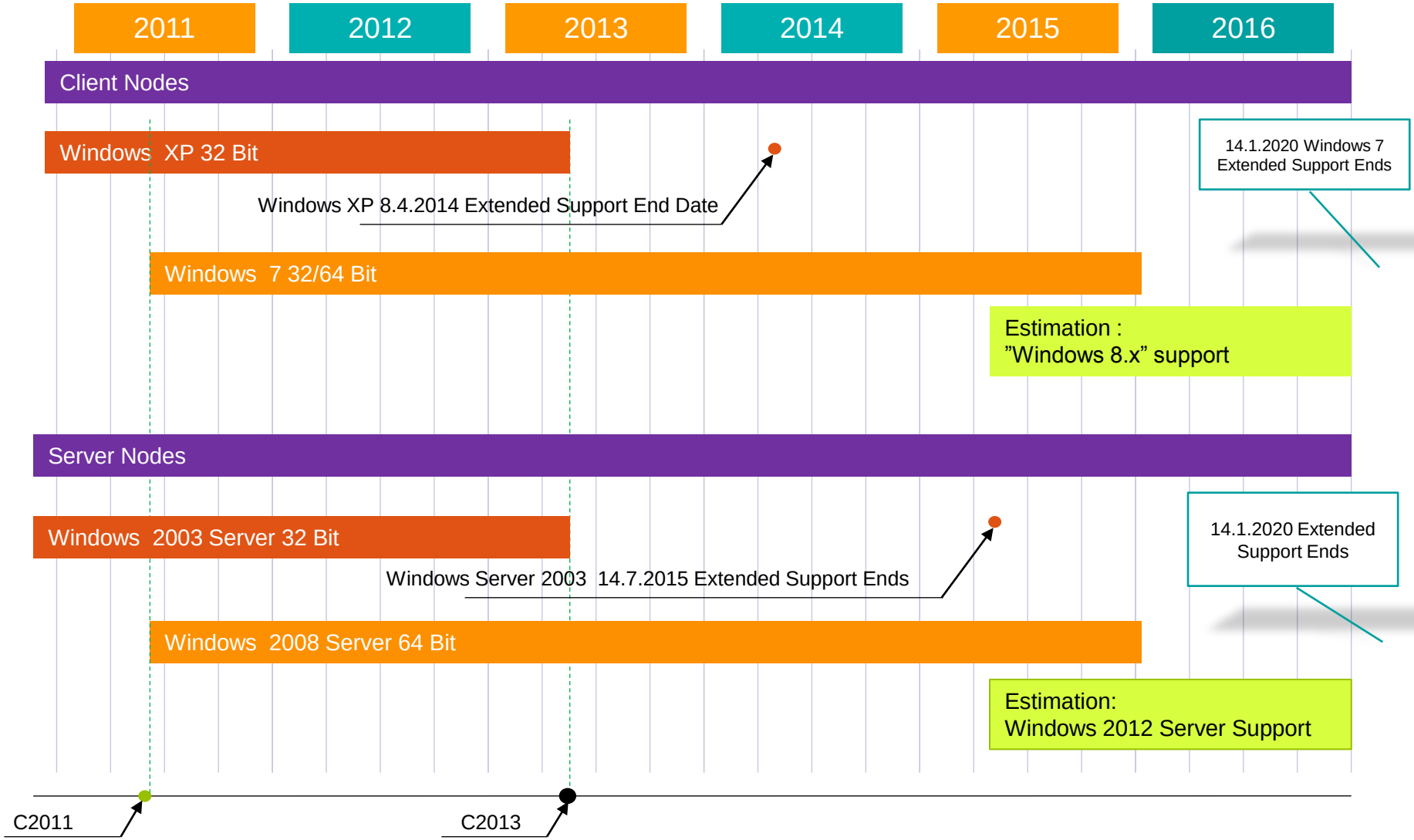


Compatible Technologies in five decades

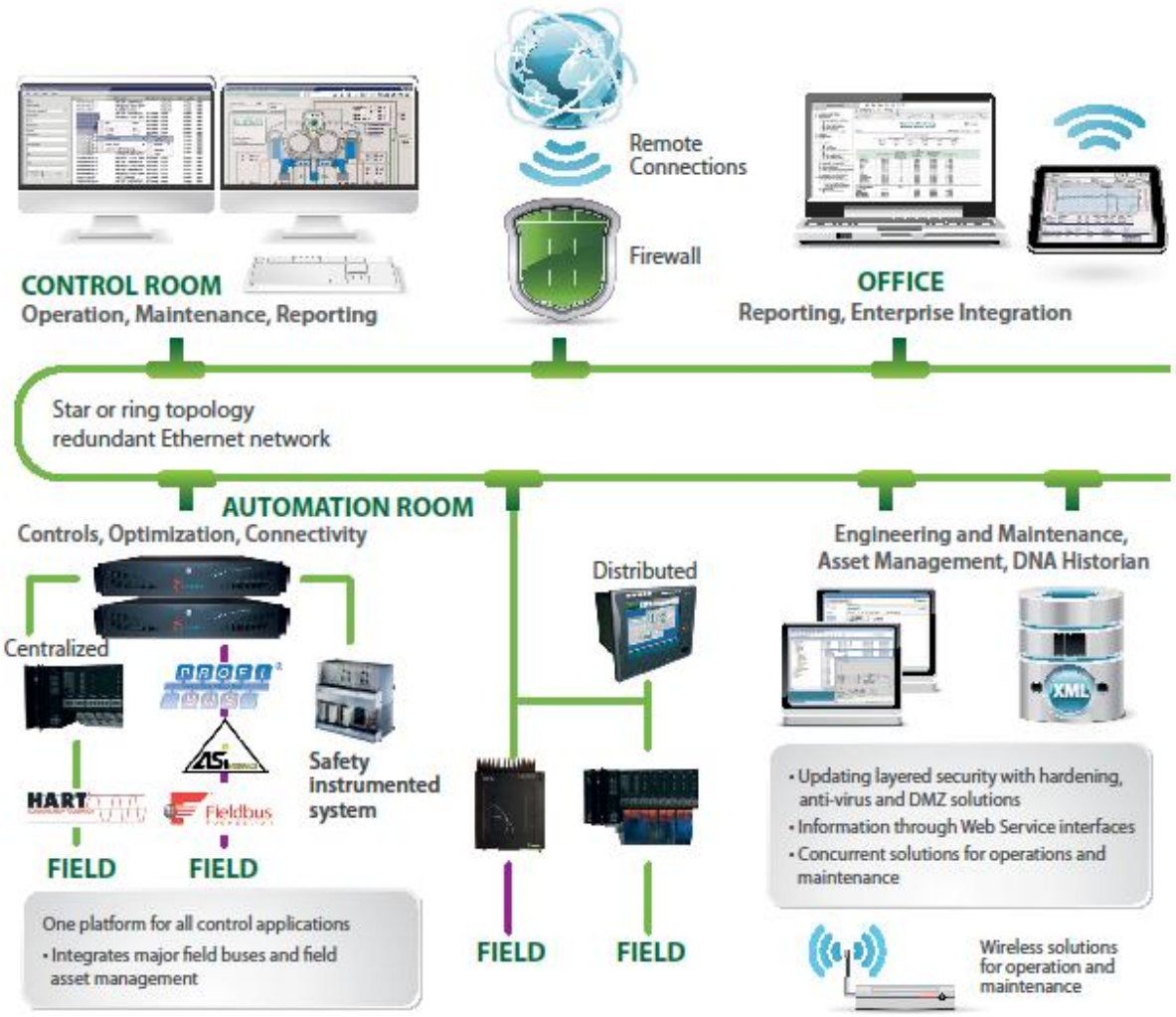
Production | Spares | Phase-out

Note: This roadmap may change due to availability of the components, technologies or other reasons.
Windows operating system Life Cycle is based on Microsoft Life Cycle Policy

Metso DNA – MS Windows OS Support

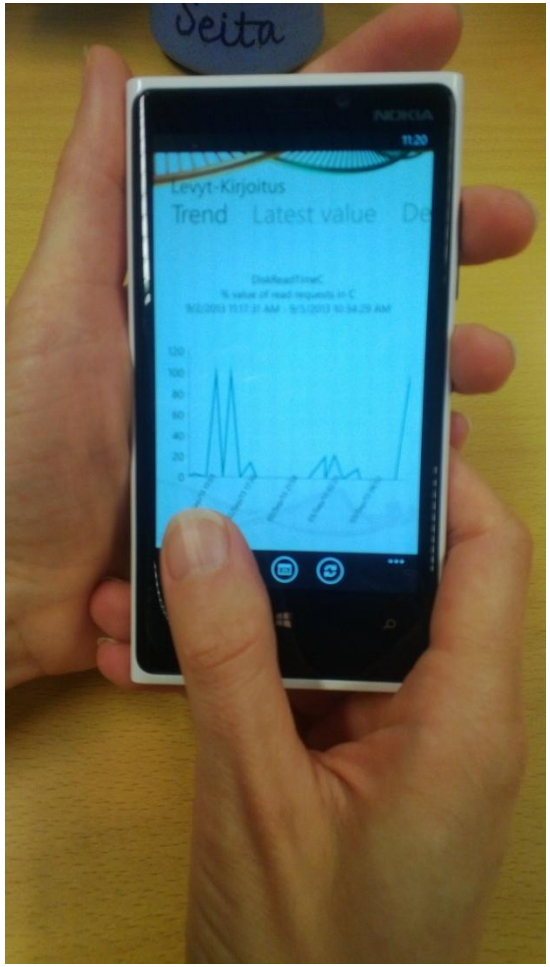


Metso DNA – General architecture



Metso DNA Smart Phone App

Looks and feels as any other app in your phone



Youtube (=> Metso DNA Windows Phone)

https://www.youtube.com/watch?v=CgvnKsb7IDo

Uhkien ja haavoittuvuuksien hallinta

Mikä erottaa tuotantoympäristön toimistoympäristöstä?

Uhkien ja haavoittuvuuksien hallinta

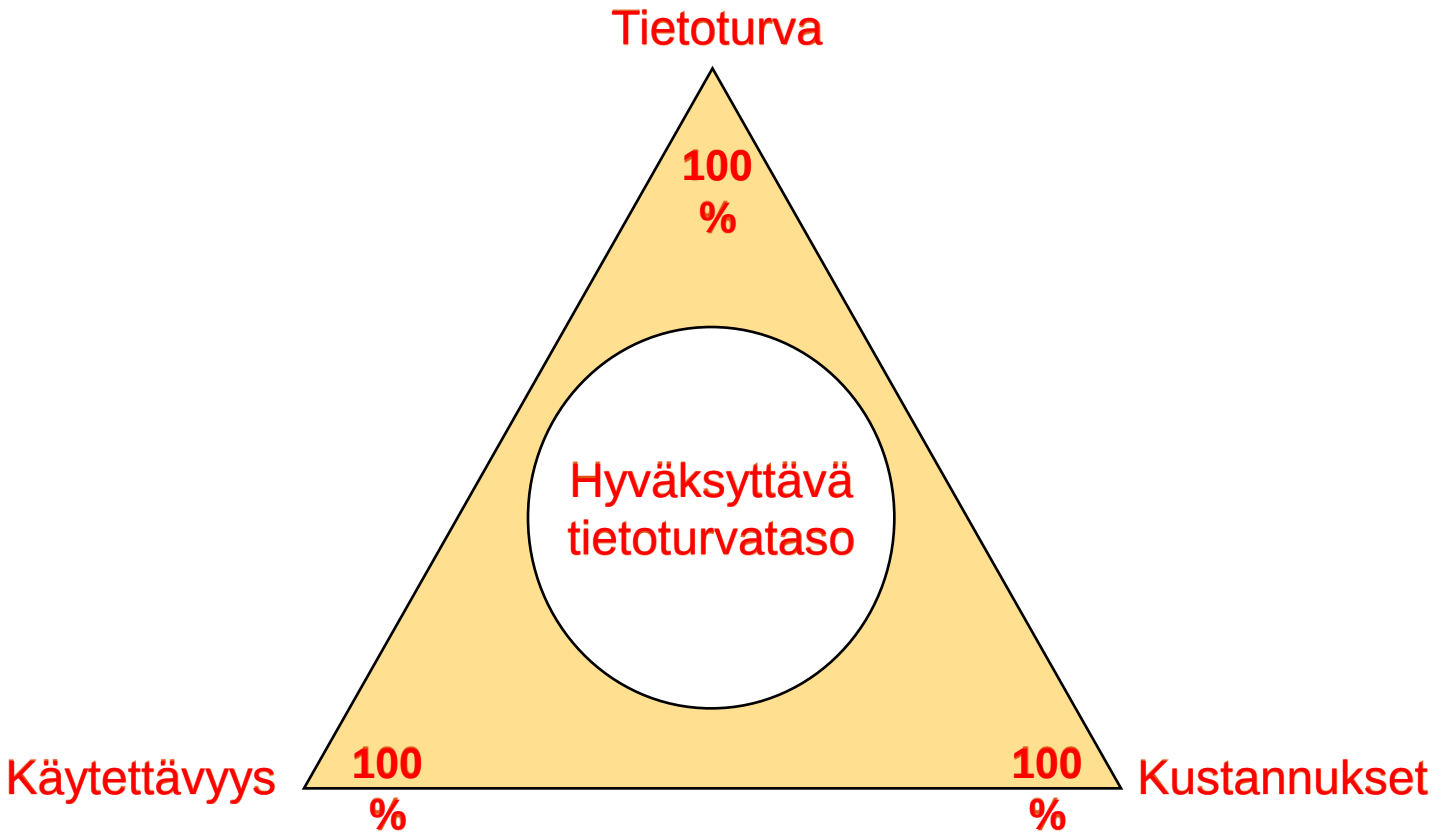
Mikä on teollisuusautomaatiojärjestelmä (ICS)?

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.

- *http://en.wikipedia.org/wiki/Industrial_Control_Systems*

Uhkien ja haavoittuvuuksien hallinta

Tietoturvan optimointi



Tietoturvan optimointi on osa riskienhallintaa

Uhkien ja haavoittuvuuksien hallinta

Tuotantoympäristö vs. toimistoympäristö

Office: Security > Availability	Production: Availability > Security
Office users •No (rigorous) real time demands •No redundancy	Process control system • Dangerous environments (life danger) • Production targets ($) • Quality, production, environmental •Rigorous real-time controls •Malfunction not to stop production •Redundancy required
COTS components (hw & sw) •Continuous, automatic updates •Booting of PCs' is not a problem •Standard workstations, servers and network solutions •100…1000…10000…	Proprietary systems •Static, automatic updates not possible •Fault not allowed to stop production •Proprietary hw&sw, embedded systems, industrial, field buses, field devices, … •Various generations •Several automation vendors •1…10…100…
Short life cycles	Long life cycles
Responsibility: IT organization	Responsibility: Production, automation maintenance organization, control system vendor

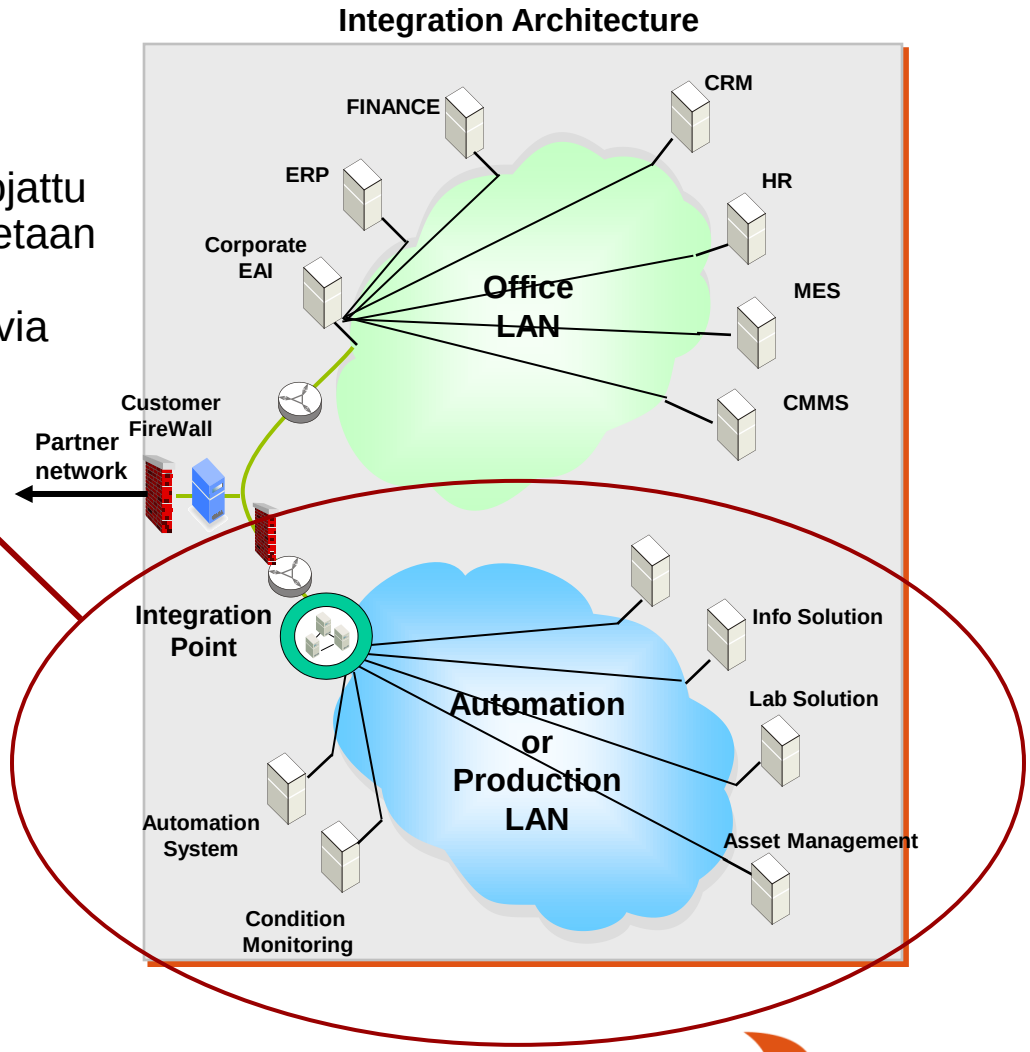
Uhkien ja haavoittuvuuksien hallinta

Tuotantoympäristö vs. toimistoympäristö

- Tuotantoympäristön tulee olla asianmukaisesti erotettu ja suojattu verkko, jolla pystytään varmistetaan tuotannon jatkuminen, vaikka toimistoverkossa ilmenisi vakavia tietoturvaongelmia

Metso Automation has a deep expertise and products inside Automation LAN

- Selkeä liityntä ylätason järjestelmiin
- Järjestelmän integraatio
- Partnereiden liityntä



Automaatio ja kriittinen infrastruktuuri

Uhkien ja haavoittuvuuksien hallinta

Kriittinen infrastruktuuri uhkien kohteena

BBC News Sport Weather Travel Culture Autos

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environm

17 August 2012 Last updated at 14:22 GMT

Share

Shamoon virus targets energy sector infrastructure

A new threat targeting infrastructure in the energy industry has been uncovered by security specialists.

Saudi Aramco is Saudi Arabia's

The attack, known as Shamoon, is said to have hit "at least one organisation" in the sector.

Shamoon is capable of wiping files and rendering several computers on a network unusable.

On Wednesday, Saudi Arabia's national oil company said an attack had led to its own network being taken offline.

Although Saudi Aramco did not link the issue to the Shamoon threat, it did

On August 15, 2012, the Saudi Arabian Oil Company (also known as Saudi Aramco), Saudi Arabia's national petroleum concern, a producer, manufacturer, marketer and refiner of crude oil, natural gas, and petroleum products,[1] was struck by a computer virus that possibly spread across as many as 30,000 Windows-based personal computers operating on the company's network. According to news sources, it may have taken Aramco almost two weeks to fully restore its network and recover from a disruption of its daily business operations caused by data loss and disabled workstations resulting from the incident. Computer security research community dubbed the virus reputed to have spread across Aramco's network Shamoon.

- http://www.bbc.co.uk/news/technology-19293797
- http://bakerinstitute.org/publications/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf

Uhkien ja haavoittuvuuksien hallinta

Automaatioympäristön haavoittuvuuksia seurataan

- Control Systems Advisories and Reports by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

ICS-CERT Alerts

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

- ICS-ALERT-13-091-01 : Mitsubishi MX Overflow Vulnerability
- ICS-ALERT-13-091-02 : Clorius Controls ICS SCADA Information Disclosure
- ICS-ALERT-13-016-01A : Schneider Electric Authenticated Communication Risk Vulnerability (Update A)
- ICS-ALERT-13-016-02 : Offline Brute-Force Password Tool Targeting Siemens S7
- ICS-Alert-13-016-01 : Schneider Electric Multiple Vulnerabilities
- ICS-ALERT-13-004-01 : Advantech Studio Directory Traversal
- ICS-ALERT-13-009-01 : Advantech WebAccess Cross Site Scripting Vulnerability
- ICS-ALERT-12-039-01 : Advantech Broadwin RPC Server Vulnerability
- ICS-ALERT-12-097-02A : 3S-Software CoDeSys Improper Access Control (Update)
- ICS-ALERT-12-046-01A : Increasing Threat to Industrial Control Systems (UPDATE A)
- ICS-ALERT-12-277-01 : Sielco Sistemi WinLog Lite SEH Overwrite Vulnerability
- ICS-ALERT-12-019-01 : GE D20ME PLC Multiple Vulnerabilities
- ICS-ALERT-12-234-01 : Key Management Errors in RuggedCom's Rugged Operating System
- ICS-ALERT-12-234-01A : Key Management Errors in RuggedCom's Rugged Operating System (Update A)
- ICS-ALERT-12-212-02 : WellinTech KingView User Credentials Not Securely Hashed
- ICS-ALERT-12-212-01 : Kessler Ellis Products Infilink HMI Insufficiently Protected Credentials
- ICS-ALERT-12-179-01 : Sielco Sistemi Winlog Multiple Vulnerabilities
- ICS-ALERT-11-343-01A : Control System Internet Accessibility (Update)
- ICS-ALERT-12-166-01 : Sielco Sistemi Winlog Buffer Overflow

ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.

- ICSA-12-354-01A : Ruggedcom ROS Hard-Coded RSA SSL Private Key Update
- ICSA-13-106-01 : MatrikonOPC Multiple Product Vulnerabilities
- ICSA-13-116-01 : Galil RIO-47100 Improper Input Validation
- ICSA-13-100-01 : Schneider Electric MiCOM S1 Studio Improper Authorization Vulnerability
- ICSA-13-098-01 : Canary Labs Inc Trend Link Insecure ActiveX Control Method
- ICSA-13-095-02 : Rockwell Automation FactoryTalk and RSLinx Multiple Vulnerabilities
- ICSA-13-095-01 : Cogent Real-Time Systems Multiple Vulnerabilities
- ICSA-13-091-01 : Wind River VXWorks SSH and Web Server Multiple Vulnerabilities
- ICSA-13-050-01A : 3S CODESYS Gateway-Server Multiple Vulnerabilities (Update A)
- ICSA-13-043-02A : WellinTech KingView KingMess Buffer Overflow (Update A)
- ICSA-13-084-01 : Siemens CP 1604 and CP 1616 Improper Access Control
- ICSA-13-067-02 : Invensys Wonderware Win-XML Exporter Improper Input Validation Vulnerability
- ICSA-13-079-02 : Siemens WinCC 7.0 SP3 Multiple Vulnerabilities
- ICSA-13-079-01 : Schweitzer Engineering Laboratories AcSELerator Improper Authorization Vulnerability
- ICSA-13-079-03 : Siemens WinCC TIA Portal Vulnerabilities
- ICSA-13-077-01A : Schneider Electric PLCS Multiple Vulnerabilities (UPDATE)
- ICSA-13-077-01 : Schneider Electric PLCS Multiple Vulnerabilities
- ICSA-13-053-02A : Honeywell Enterprise Buildings Integrator (EBI) Symmetre and ComfortPoint Open Manager Station (Update A)
- ICSA-13-053-01 : Emerson DeltaV Uncontroller Resource Consumption Vulnerability

- http://ics-cert.us-cert.gov/

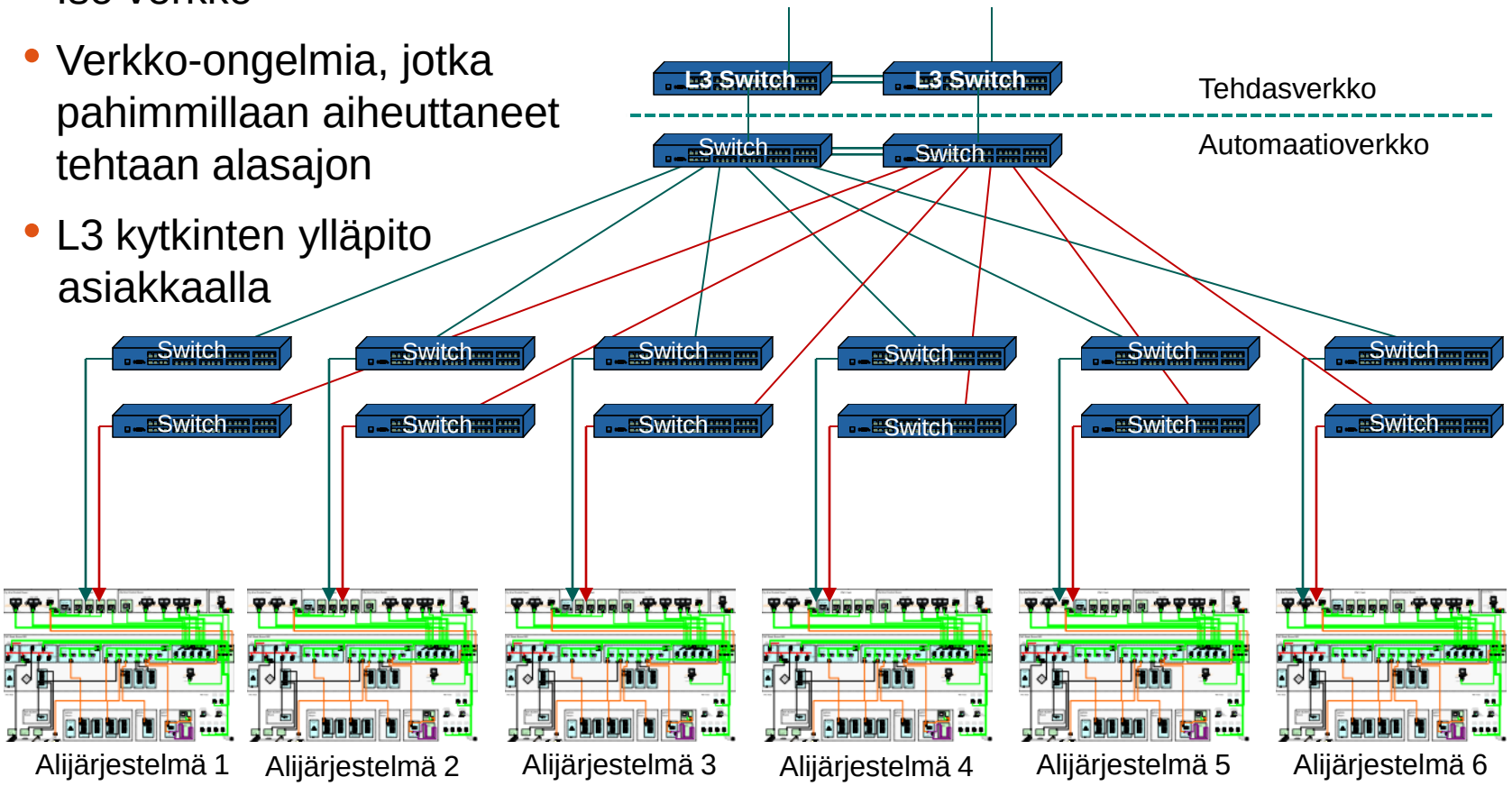
Case Study

Automaation tietoverkkojen hallinta

Case study:Automaation tietoverkkojen hallinta

Lähtötilanne

- Iso verkko
- Verkko-ongelmia, jotka pahimmillaan aiheuttaneet tehtaan alasajon
- L3 kytkinten ylläpito asiakkaalla



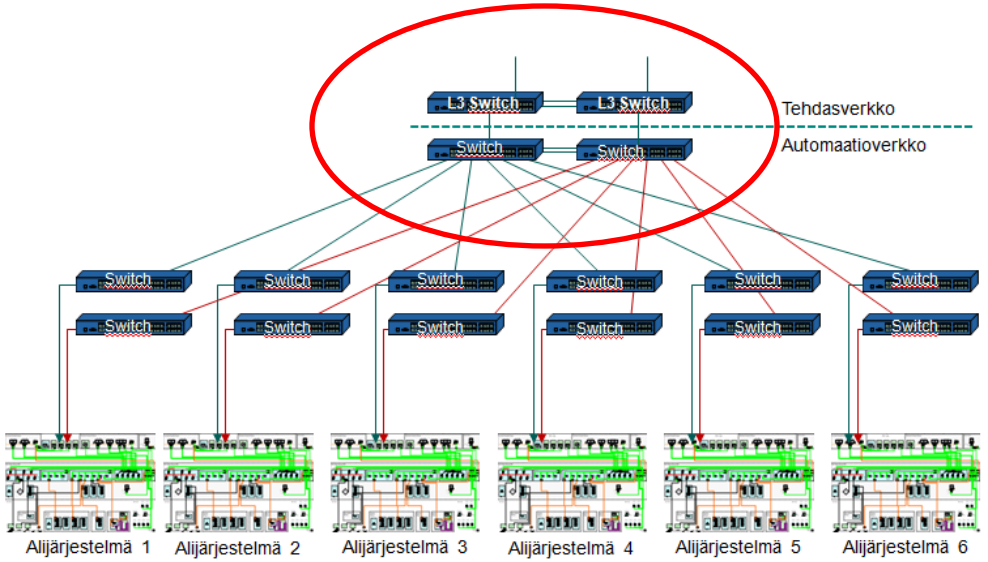
Case study:Automaation tietoverkkojen hallinta

Analyysi

- Automaatioverkon eristämistä ei tehty asianmukaisesti
- Rajoittamaton liikenne automaatiojärjestelmän ja tehdasverkon välillä
- Automaatiotoimittajan suositukset korvattu tehtaan IT osaston suosituksilla (L3 tason kytkimen konfiguraatio ristiriidassa DCS-verkon konfiguraation kanssa)

➡ Verkkomyrskyjä

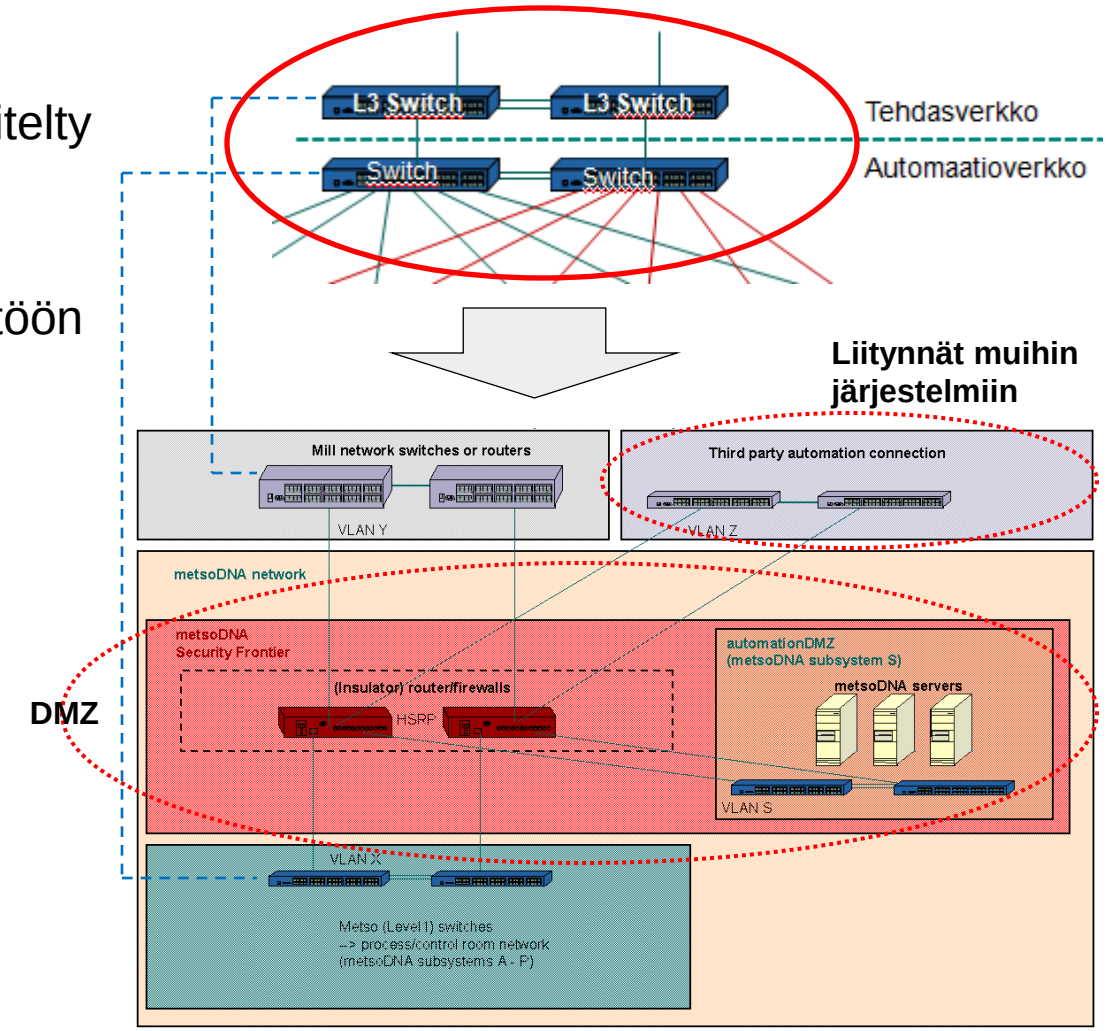
➡ Tietoturva ja käytettävyysriski



Case study:Automaation tietoverkkojen hallinta

Korjaavat toimenpiteet

- Verkkojen eristäminen määritelty ja verkon konfigurointi tehty asianmukaisesti
- Reititinpalomuuri otettu käyttöön
- Luotu erillinen DMZ (demilitarisoitu) alue automaatiojärjestelmän ja tehdasverkon välille



Case study:Automaation tietoverkkojen hallinta

Opetukset

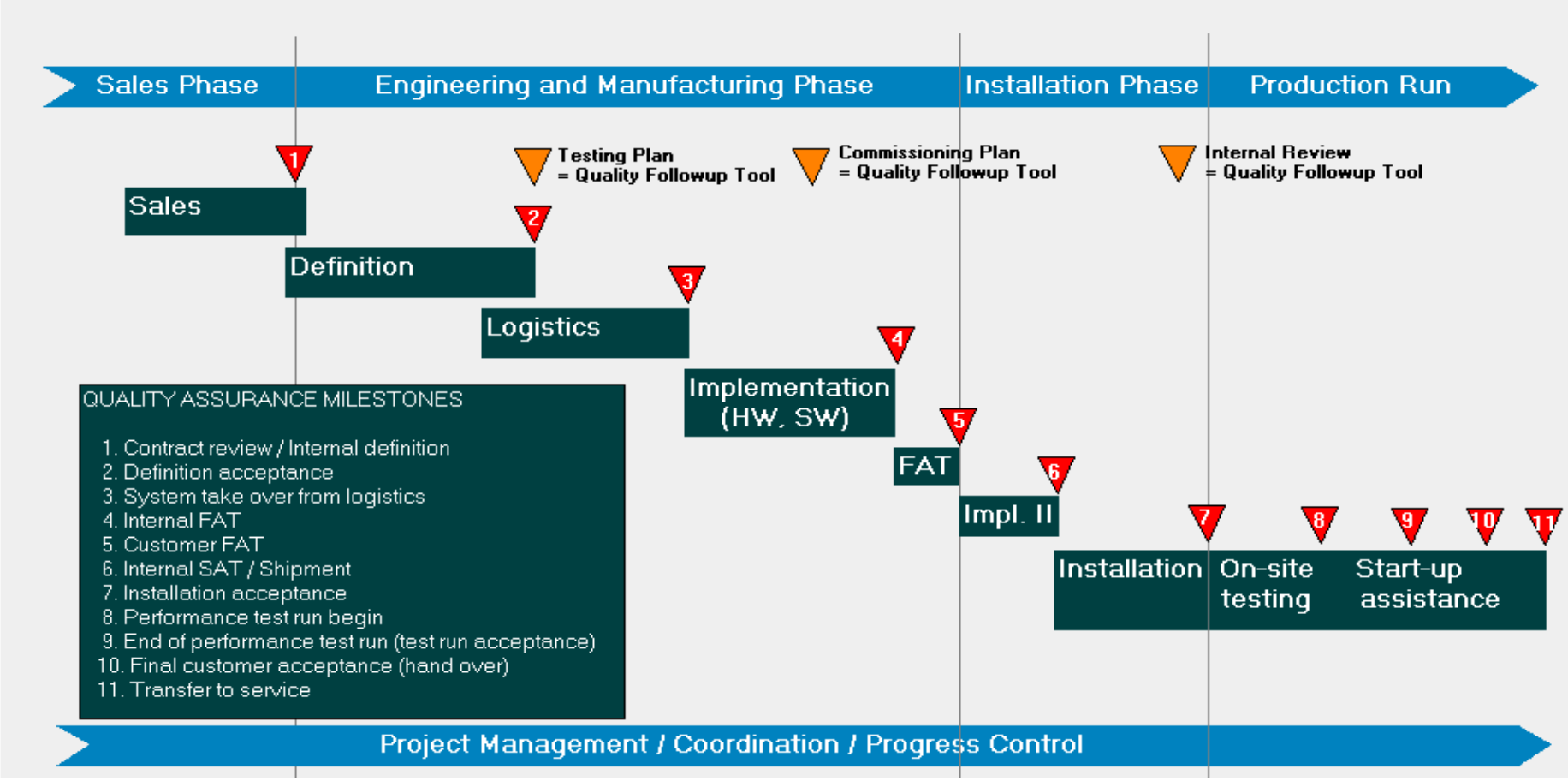
- Automaatiojärjestelmän liittäminen tehdasverkkoon tehtävä asianmukaisesti
- Mahdolliset erilliset tietoturvaa parantavat ratkaisut myös mietittynä (IDS/IPS, DMZ alueen käyttöönotto, jne.)
- Tehtaan IT mukana jo projektin alkuvaiheesta lähtien, jotta mahdolliset ristiriidat saadaan ratkaistua siten, että järjestelmän käytettävyys ja tietoturva ovat riittävällä tasolla

Uhkien ja haavoittuvuuksien hallinta

Korkean käytettävyyden varmistaminen toimitusprojektissa

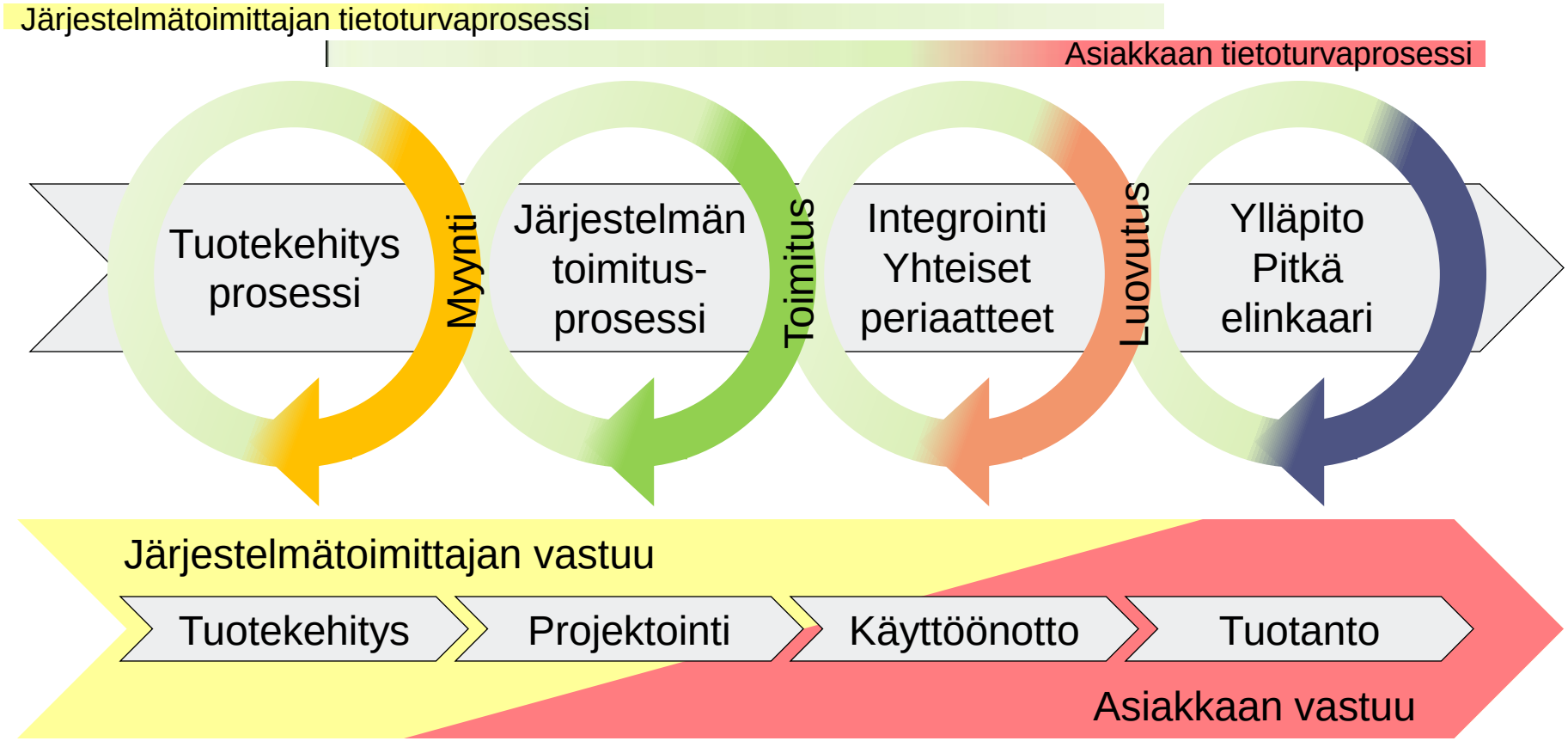
Uhkien ja haavoittuvuuksien hallinta

Automaatiotoimituksen eteneminen



Uhkien ja haavoittuvuuksien hallinta

Vastuut



Hardening Windows operating systems

Metso Automation	Guide	1 (31)
PAS	Ready	INTERNAL
Systems RTD	22.8.2011	46bb.1.1

It is quite detailed

Hardening Windows Server 2008 for Metso DNA

CONTENTS

Antivirus Software

Symantec Endpoint Protection (SEP) v12

One year antivirus software licence included in all new Metso DNA system installations

-> To keep the system security up-to-date throughout the delivery project

-> Good basis to continue Security Follow-Up after the delivery project

Uhkien ja haavoittuvuuksien hallinta

Korkean käytettävyyden varmistaminen

- Tietoturva varmistamassa korkeaa käytettävyyttä
  - Verkkoarkkitehtuuri (verkkojen erotus, verkkolaitteiden konfigurointi, DMZ-ratkaisun käyttö)
  - Etäyhteydet
  - Käyttäjien hallinta (Active Directoryn käyttö?)
  - Endpoint security (tietoturvapäivitykset, virustorjunta, koventaminen)
  - Monitorointi ja ilmoitukset (Monitoring and messaging)
  - Tietoturvan hallinta
  - Palautusten suunnittelu ja hallinta (Recovery planning)
  - Tietoturvaprosessit
  - jne.

Uhkien ja haavoittuvuuksien hallinta

Automaatiojärjestelmien tietoturvatestaus

- Metso Automaation tuotekehitys ja tuotekehityksen järjestelmätestaus suunnittelee, kehittää, testaa ja ylläpitää tietoturvaa:

→ dedikoitu ”Security Team”; koottu henkilöistä automaation järjestelmäkehityksen eri osa-alueilta

  - Seuraa yleisesti tilannetta eri kanavista (CERT-FI, ICS-CERT, Microsoft, …)
  - Tarkastaa ja testaa/testauttaa päivitykset (laitefirmwaret, käyttöjärjestelmät, …)
  - Tiedottaa suosituksista ja toimittaa päivitykset jakeluun
  - Tutkii ja kehittää ratkaisuita tietoturvan kehittämiseksi
    - DMZ ratkaisut, etäkäyttöratkaisut, palomuurien aukaisulistat, laitekovennukset, IDS/IPS, ohjeistukset menetelmiin, parametrointiin ja testaukseen, …

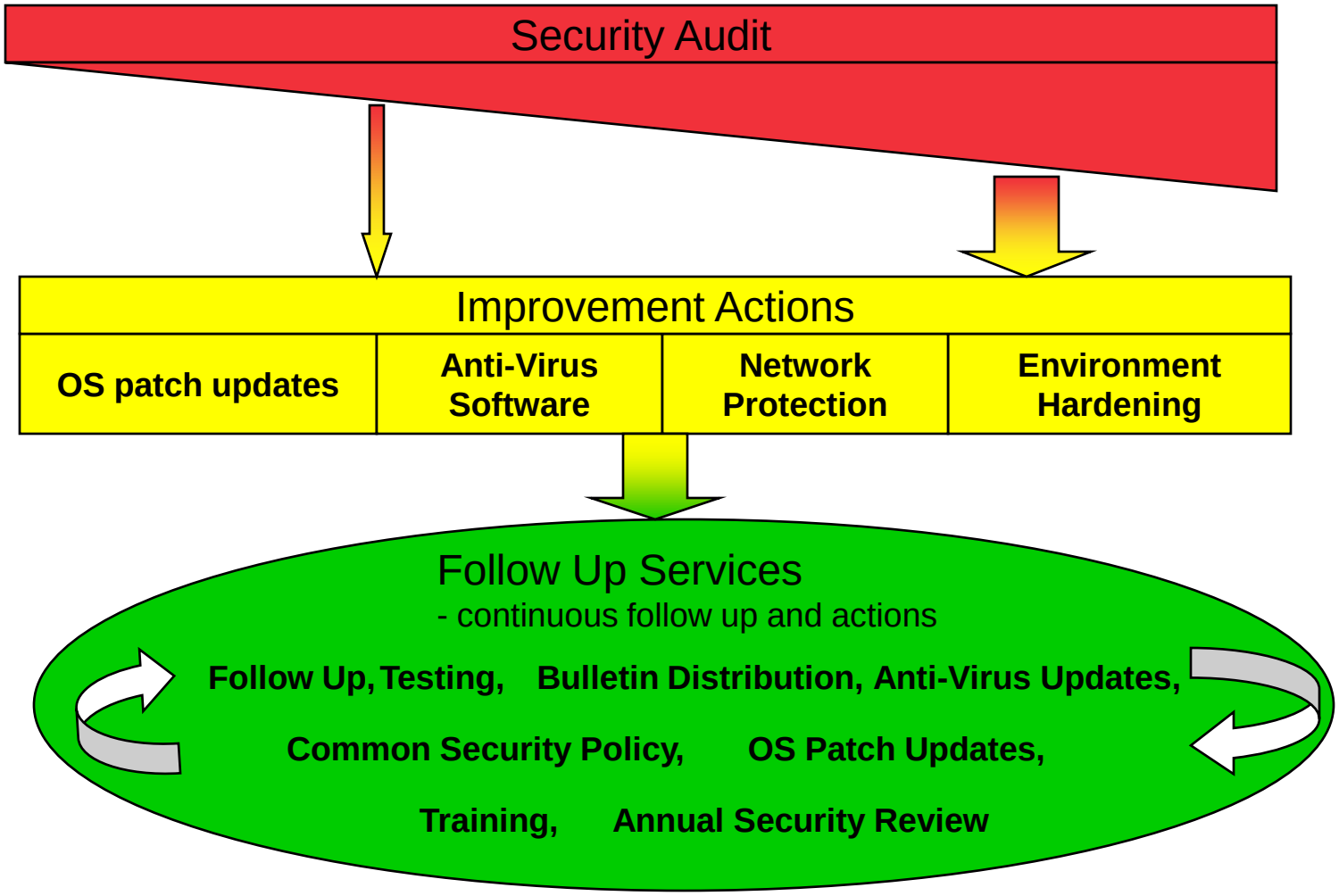
- Projektointi ja Asiakaspalvelu toteuttavat annettuja suosituksia

Security Services

Keep Metso DNA system security up-to-date

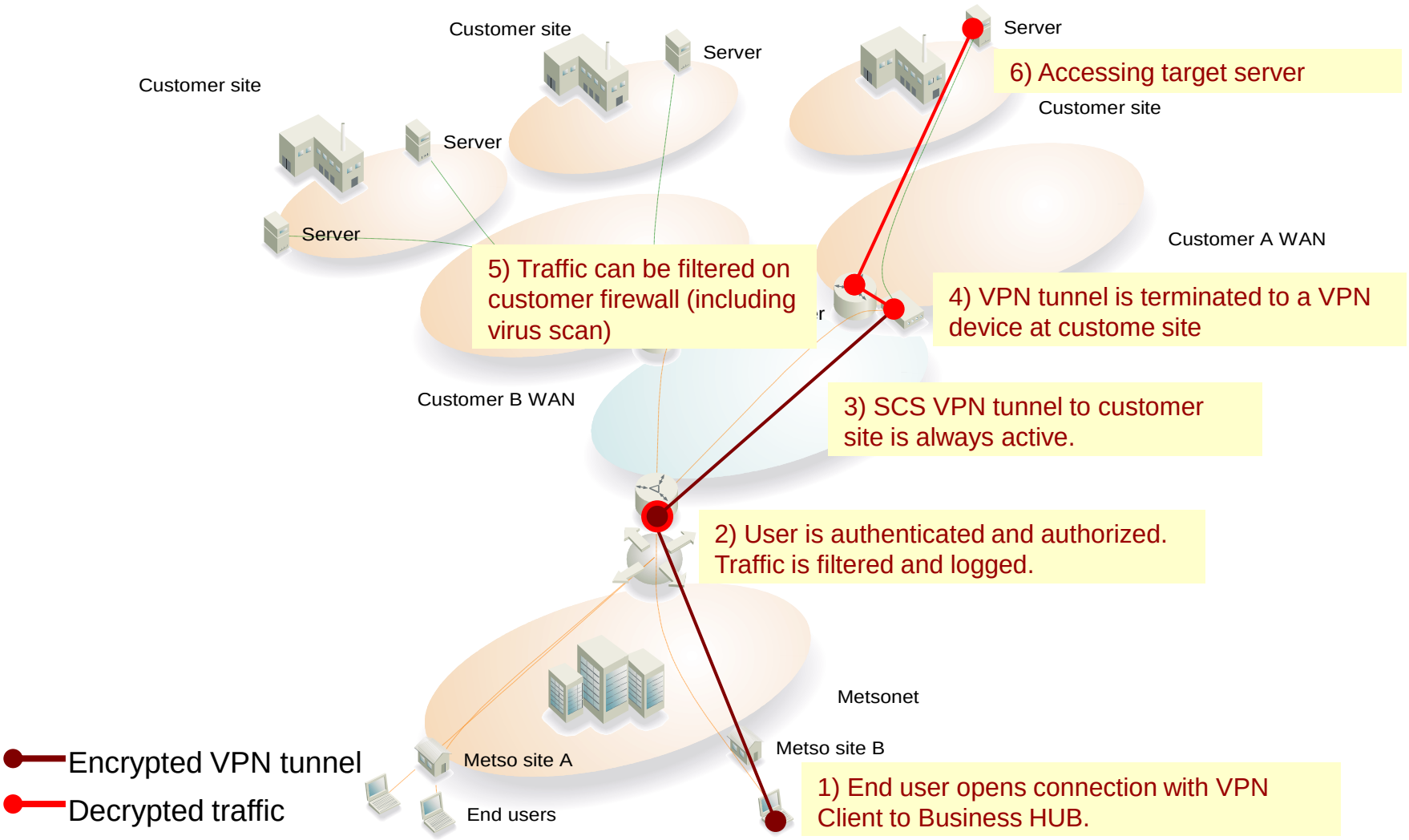
metso

Metso DNA Security Services



Metso Secure Connection Solution (SCS)

Antivirus description files distributed via metso SCS connection



Security throughout the System Life Cycle

Security Follow-Up as part of holistic solution

NEW INSTALLATION
- ✓ Network architecture
- ✓ Remote connections
- ✓ Hardening

DISASTER MANAGEMENT
- ✓ Continuous backups
- ✓ Fast recovery plan

SECURITY TRAINING

SECURITY FOLLOW-UP
Up-to-date and tested ...
- ✓ **antivirus software**
- ✓ **antivirus descriptions**
- ✓ **security patches**

ANNUAL SECURITY AUDIT
- ❑ Checking status of ...
- ✓ OS support for Win-nodes
- ✓ antivirus software & security updates

- ❑ Proactive planning of ...
- ✓ OS upgrades to PCs, servers and switches
- ✓ replacement of switches

NETWORK STUDY *)
- ❑Analysis of network ...
- ✓ security
- ✓ availability
- ✓ performance
- ✓ scalability

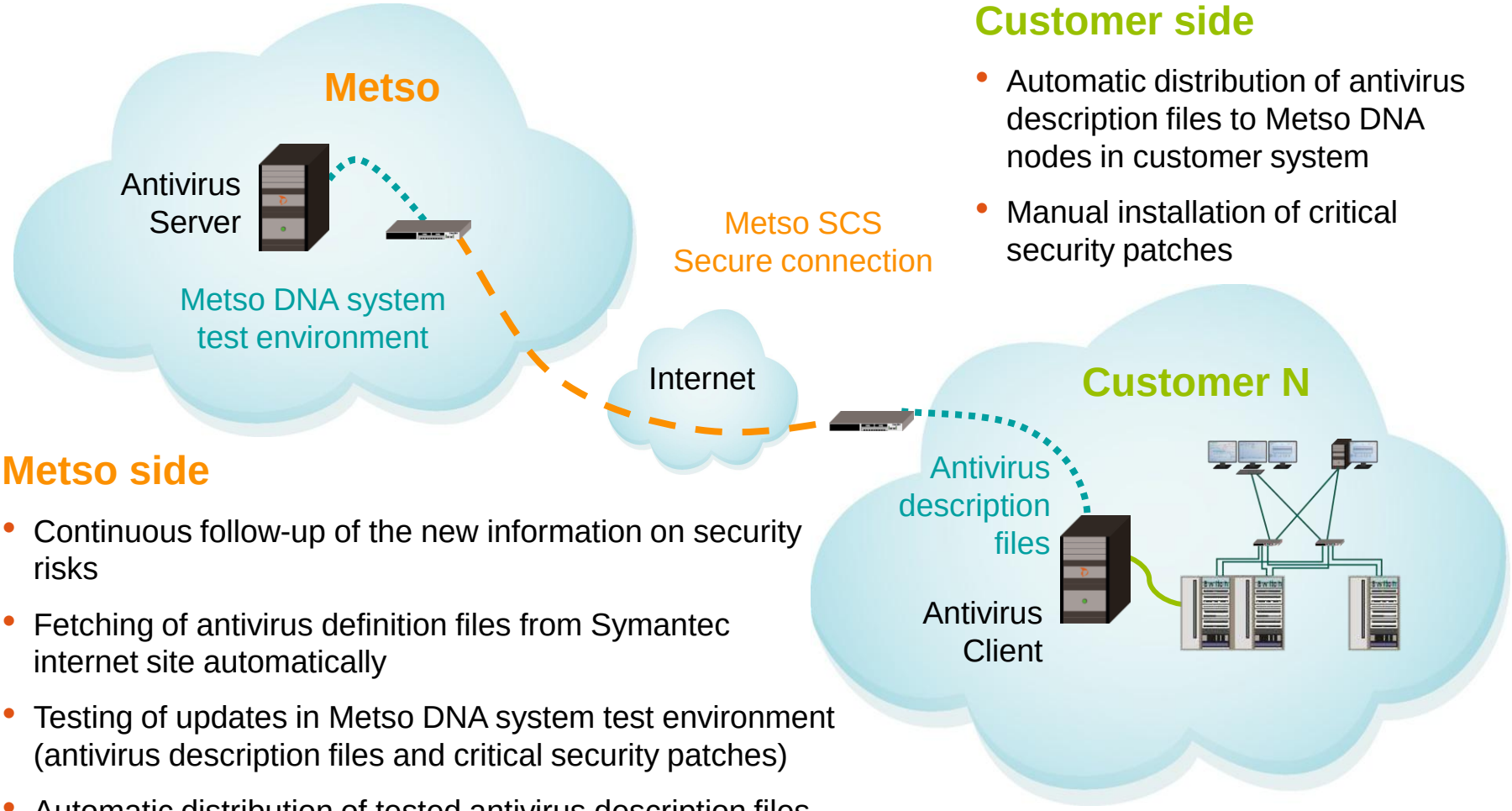
- ❑Installation of Network Monitoring tool

- ❑Proactive planning of ...
- ✓ improvements/upgrades in network structure

*) Recommended every 2-3 years. Always before expanding the existing system with a new subsystem or annual audit reveals possible bottlenecks/risks or there are symptoms of network problems.

Security Follow-Up

Continuous battle against new worms and viruses



Customer side

- Automatic distribution of antivirus description files to Metso DNA nodes in customer system
- Manual installation of critical security patches

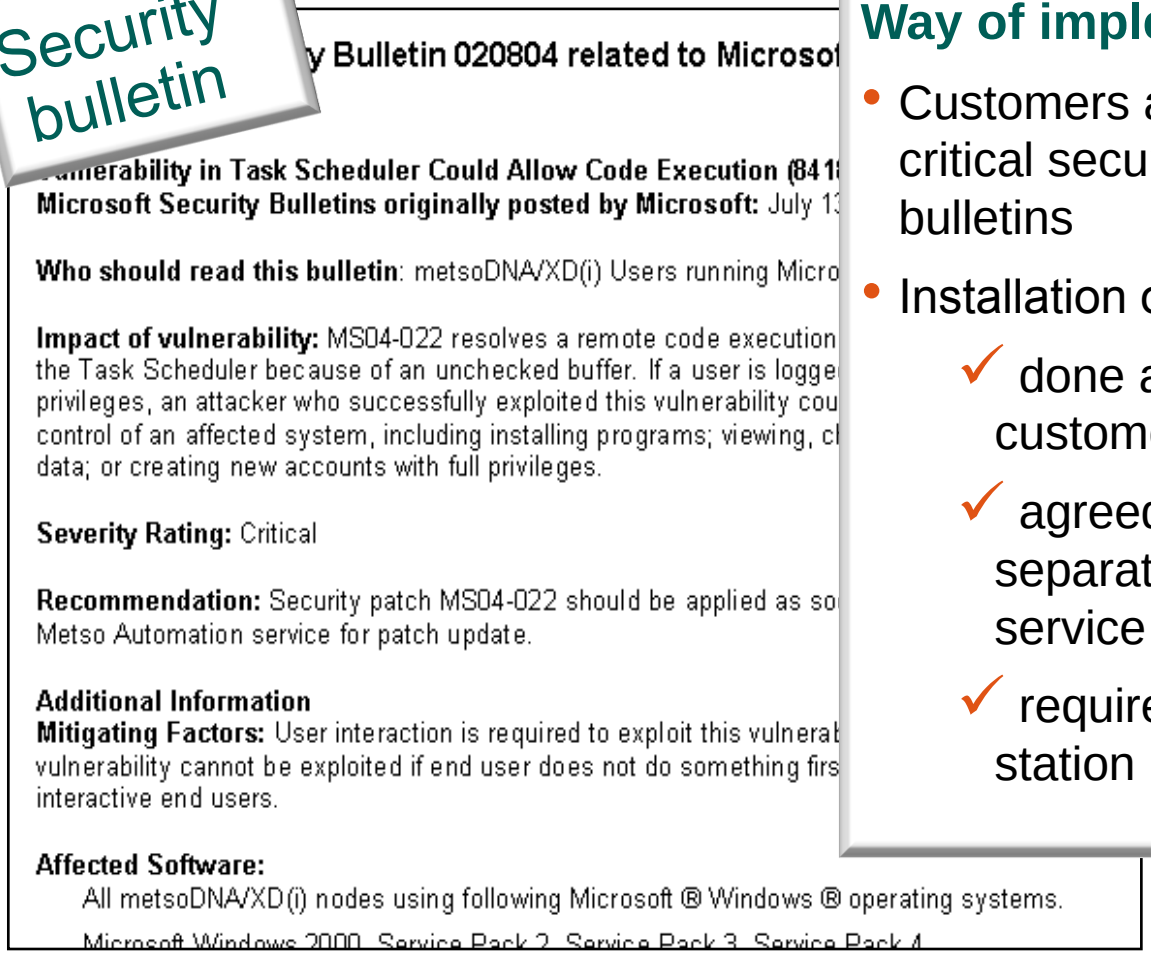
Metso side

- Continuous follow-up of the new information on security risks
- Fetching of antivirus definition files from Symantec internet site automatically
- Testing of updates in Metso DNA system test environment (antivirus description files and critical security patches)
- Automatic distribution of tested antivirus description files to customers (Antivirus Client) everyday at 7pm (Mon-Fri)

Security Patches

Rapid response to potential critical risks

Security bulletin



…y Bulletin 020804 related to Microsof

…lnerability in Task Scheduler Could Allow Code Execution (841…
Microsoft Security Bulletins originally posted by Microsoft: July 1…

Who should read this bulletin: metsoDNA/XD(i) Users running Micro…

Impact of vulnerability: MS04-022 resolves a remote code execution … the Task Scheduler because of an unchecked buffer. If a user is logge… privileges, an attacker who successfully exploited this vulnerability cou… control of an affected system, including installing programs; viewing, c… data; or creating new accounts with full privileges.

Severity Rating: Critical

Recommendation: Security patch MS04-022 should be applied as so… Metso Automation service for patch update.

Additional Information
Mitigating Factors: User interaction is required to exploit this vulnerab… vulnerability cannot be exploited if end user does not do something firs… interactive end users.

Affected Software:
All metsoDNA/XD(i) nodes using following Microsoft ® Windows ® operating systems.
Microsoft Windows 2000 Service Pack 2 Service Pack 3 Service Pack 4

Way of implementation

- Customers are informed about critical security patches by security bulletins
- Installation of security patches …
  - ✓ done as manual work at customer site
  - ✓ agreed and invoiced separately based on the valid service price list
  - ✓ requires shut down because station needs to be reset

metso

Security Follow-Up
Scope of supply

Item	Included	Responsible
Antivirus Server HW & SW	Yes	Metso
Installation and maintenance of Antivirus Server HW & SW in customer site	Yes	Metso
AV software licenses and updates	Yes	Metso
Continuous follow-up of the new information on security risks	Yes	Metso
Functional testing of antivirus definition files in Metso DNA test environment	Yes	Metso
Automatic distribution of antivirus definition files to customer Metso DNA nodes (Mon – Fri 7 pm)	Yes	Metso
Selecting appropriate security patch updates for functional testing in Metso DNA test environment	Yes	Metso
Informing the customer about critical security patches	Yes	Metso
Installing the critical security patches in customer site	No	Metso *)

*) Agreed and invoiced separately, according to the valid price list

Coming next in ICS Security

Metso DNA Security

Increased need for security

- Security awareness increasing
  - Standards development
    - NERC-CIP
    - IEC 62443 [ANSI/ISA-99]
    - WIB Process control Domain: security requirements for vendors
  - Recommendations
    - NIST Special Publications
    - SCADA and Control Systems Procurement Language, DHS and ICS-CERT
  - Customer in Finland participating in security development and research projects (COREQ-VE, COREQ-ACT, Industrial Security Workshops, ...)
  - Increasing security requirements from many customer corporations
    - Security audits by external companies

→ Customers' security awareness increasing

Metso DNA Security

Ongoing new actions

- Intrusion Detection and Protection Systems to strengthen DMZ
- White listing instead of antivirus scanners
  - Proactive monitoring and protection for physical and virtual server environments
- Solving virtualization, mobile (3G) and cloud security concerns together with customer IT
- Partnering with IT security technology companies (and other research partners) to be able to supply bigger security scopes.

metso

Expect results