SIEMENS
Ingenuity for life

Plant Security Services – Kyberturvakartoitus

Automaatioseuran Turvallisuusjaoston automaation tietoturva –teemapäivä
10.5.2017

Plant Security Services
Digitalisaation mahdollistaja

SIEMENS

Hallitut kyberturvapalvelut mahdollistavat nopean reagoinnin, asiakkaan tiedottamisen, sekä toimenpidesuositusten ja päivityspalveluiden tuottamisen

Plant Security Service portfoliossa yhdistyvät automaatioteknologian ja syvällisen kyberturvaosaamisen korkeatasoinen asiantuntemus

'State-of-the-art' teknologiaratkaisut sekä tietoturvanormien ja standardien mukainen todennettu lähestymistapa

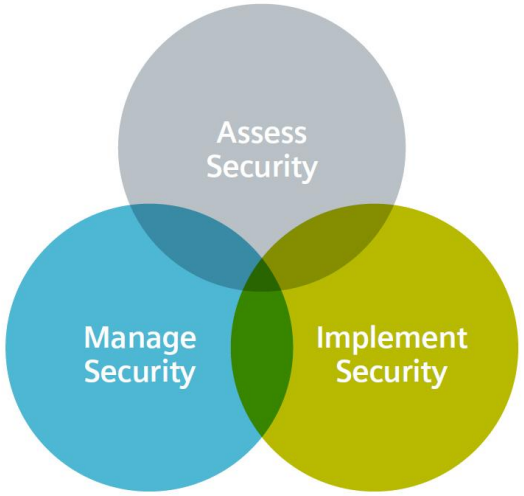
Toimialaspesifinen, kattava ja modulaarinen kyberturvaportfolio mahdollistaa räätälöityjen palveluiden toteuttamisen ja kustannustehokkuuden

Plant Security Services
Holistic approach aligned with risk management methodology

SIEMENS

Assess Security
Evaluation of the current security status of an ICS environment

Manage Security
Comprehensive security through monitoring and proactive protection



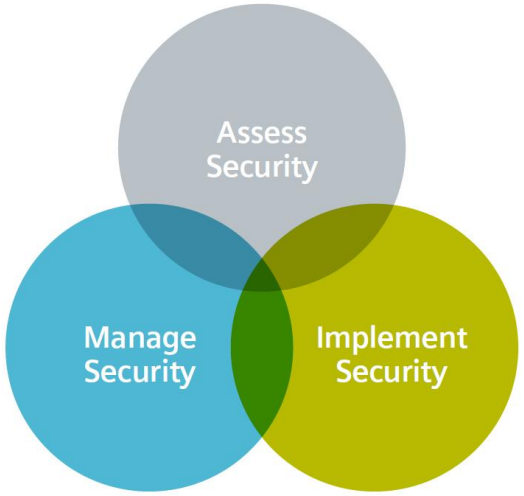
Implement Security
Risk mitigation through implementation of security measures for reactive protection

Plant Security Services
Overview of modular portfolio

SIEMENS

- IEC 62443 Assessment
- SIMATIC PCS 7 and WinCC Assessment
- Risk and Vulnerability Assessment

- Industrial Security Monitoring
- Remote Incident Handling
- Perimeter Firewall Management
- Perimeter Firewall Review
- Anti Virus Management
- Whitelisting Management
- Patch and Vulnerability Management



- Security Awareness Training
- Security Policy Consulting
- Network Security Consulting
- Perimeter Firewall Installation
- Clean Slate Validation
- Anti Virus Installation
- Whitelisting Installation
- System BackUp
- Windows Patch Installation

Plant Security Services
IT Security vs. Industrial Security

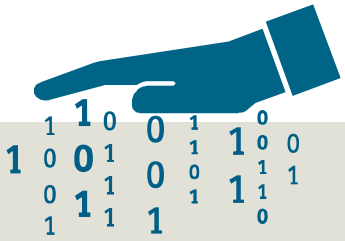
SIEMENS

Miksi kyberturvakaroitus?

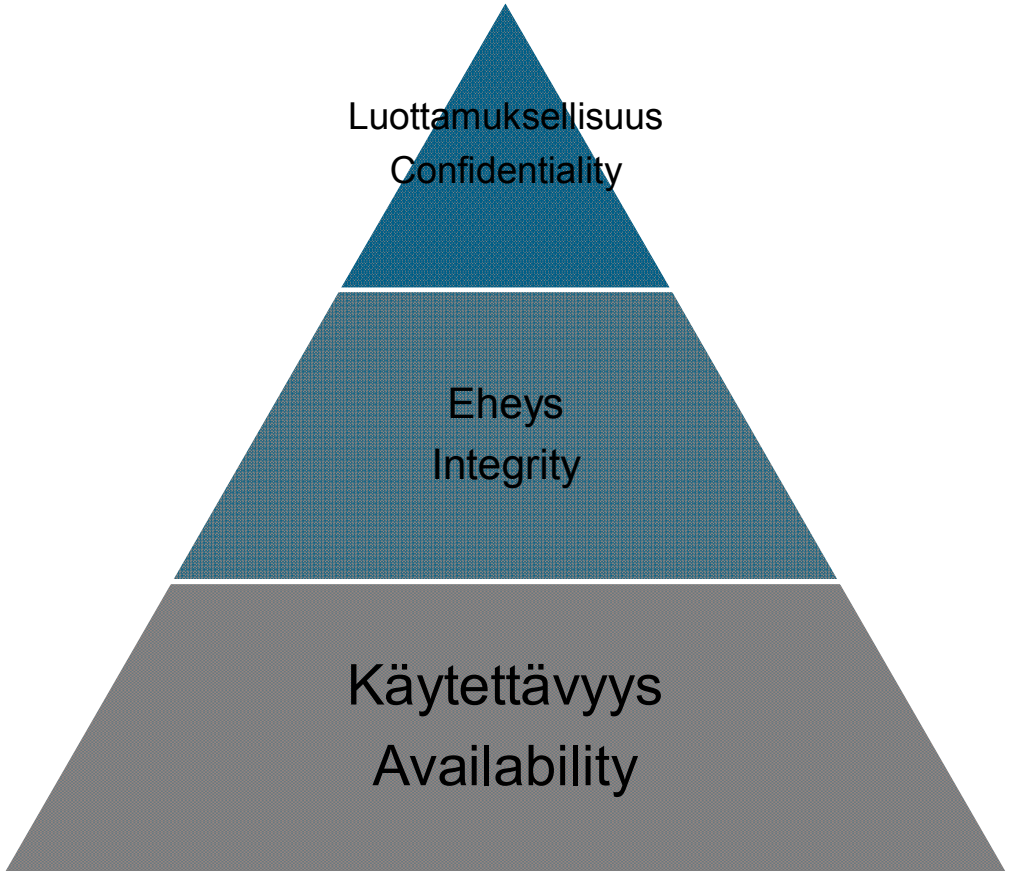
- Tietoisuus
- Riskien hallinta

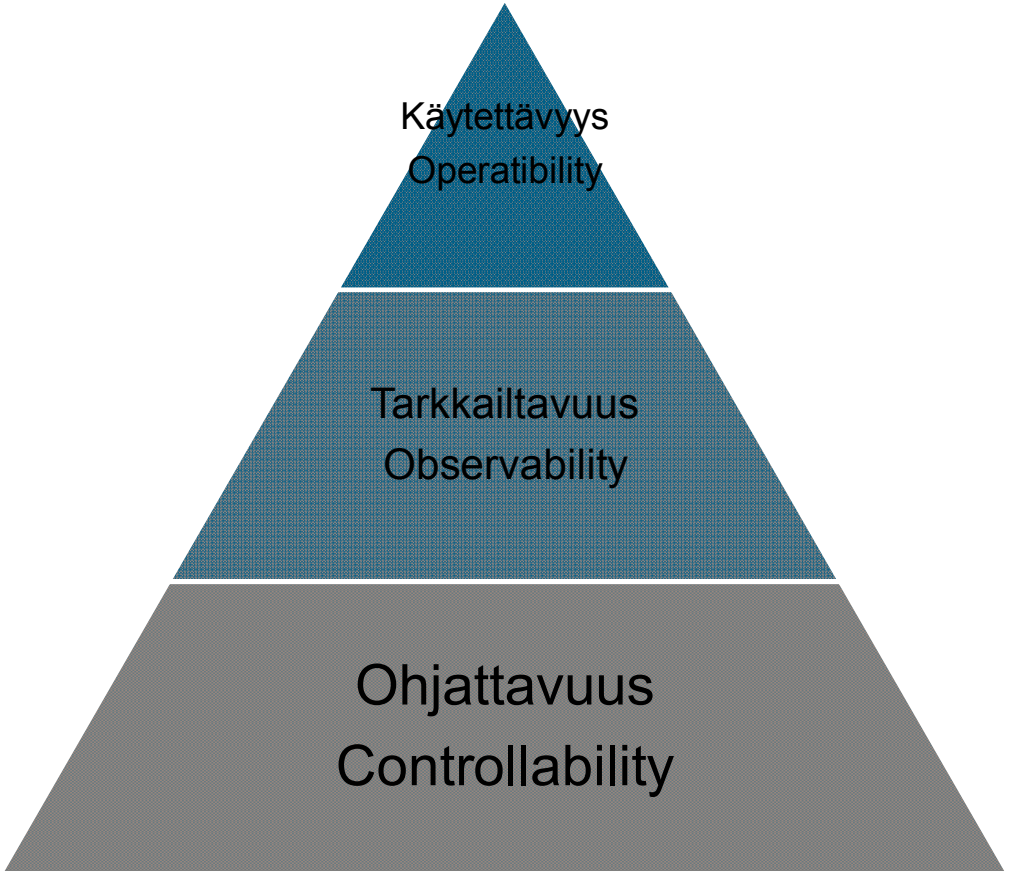
ICS Security
Teollisuusautomaatio OT vs. IT

SIEMENS

IT-Tietoturva		Teollisuusautomaation tietoturva
Luottamuksellisuus Eheys Käytettävyys		**Käytettävyys** Eheys Luottamuksellisuus
1s – 60s häiriö toleranssi on vielä hyväksyttävissä	**Käytettävyys**	Järjestelmäverkon häiriöaikatoleranssi < 300 ms
Verkko- ja tietoliikenneyhteyksien ammattilainen	**Asentaminen**	Laitoksen käyttöönottohenkilökunta
‚Tähti' - topologia	**Topologia**	Laitoskohtainen topologia
Puhdas ja ilmastoitu toimistoympäristö	**Käyttöympäristö**	Vaativa teollisuusympäristö
Suuri, kytkimissä on tyypillisesti paljon portteja	**Laitemäärä**	Pieni, kytkimissä on tyypillisesti vähemmän portteja
2-3 vuotta	**Ratkaisun elinkaari**	Minimissään 5-15 vuotta

ICS Security
Vaihtoehtoinen CO2 malli





Safety & Security
Main differences

SIEMENS

Safety protects People & Process & Environment against a machine or plant

- malfunction of machine or plant or process
  - safe reaction through limit monitoring
- mostly dedicated to internal malfunction of systems
  - high self diagnostic coverage
- possible misuse of systems if reasonably possible
  - to avoid dangerous situation during operation

Security protects a machine or plant against cyber attacks

- intentional misuse of system by applicative means
  - stop the CPU, incorrect behavior of functions
- mostly dedicated to external malfunction of systems
  - diagnostic coverage generally not implemented
- focused on misuse of systems
  - create a dangerous or not specified situation

Standards

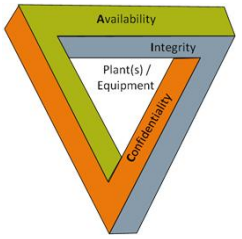
IEC 61508, IEC 61511, ISA 84 …

Standards

ISA 99, ISA/IEC 62443, WIB, NERC-CIP …

ISA 84
IEC 61508
IEC 61511

ISA 99 / IEC 62443



IEC 61511-1 Edition 2.0

8.2.4 A security risk assessment shall be carried out identify the security vulnerabilities of the SIS.

NOTE 1 Guidance related to SIS security is provided in **ISA TR84.00.09**, ISO/IEC 27001:2013, and **IEC 62443-2-1:2010**.

SIEMENS

Miksi sitten tehdään kartoitus eikä riskianalyysi/hallinta ohjelma?

- Aika ja kustannus paine
- Turvallisuus on prosessi
- Kartoituksessa huomataan perusongelmia ja saadaan tietoisuus
- Suoraviivainen aloitus antaa pohjan syventävälle jatkolle

Turvallisuudessa on kyse tasapainosta ja se on jatkuva prosessi

SIEMENS

Miksi ei tehdä penetraatiotestausta ja verkkoskannauksia?

- Vanhemmat automaatiokomponentit eivät välttämättä selviydy
- Onko kaikesta muusta jo huolehdittu
- Turvallisuustoiminnalisuuksien automaattinen testaus korkemmilla tasoilla teknisenä vaatimuksena
- Resurssikilpailu

Turvallisuudessa on kyse tasapainosta ja se on jatkuva prosessi

IEC 62443 Assessment
Overview

SIEMENS

We assess your security posture based on IEC62443

We assess in detail your security posture based on the international standard IEC62443
With the parts 3-3 “Security for industrial process measurement and control – Network and system security”
and 2-1 “Establishing an industrial automation and control system security program”

Enable you making informed decisions on the direction of their security architecture!

Processes

- We evaluate the maturity of organizational processes and work instructions towards cyber security risk mitigation

Technology

- We evaluate your installed base and system architecture to find gaps regarding the IEC standard

Deliverables

- IEC62443 gap report
- Recommendations for risk mitigation controls
- Roadmap (standardized) of how to implement cyber security

IEC 62443 Assessment
Objectives

SIEMENS

Primary objectives and key success metrics

- **IEC62443 security gap check**
- **What is the current overall security risk/threat situation of your production networks and systems?**
- **Are the production networks and systems currently exposed to cyber attacks or risks that stakeholders are unaware of?**
- **Are the current site security policies/procedures adequate to protect it against the latest and emerging threats?**
- **What are the improvement potential areas and how can the site security level be improved?**
- **And how can this enhanced security level be continuously kept up afterwards?**

IEC 62443 Assessment
Deliverables

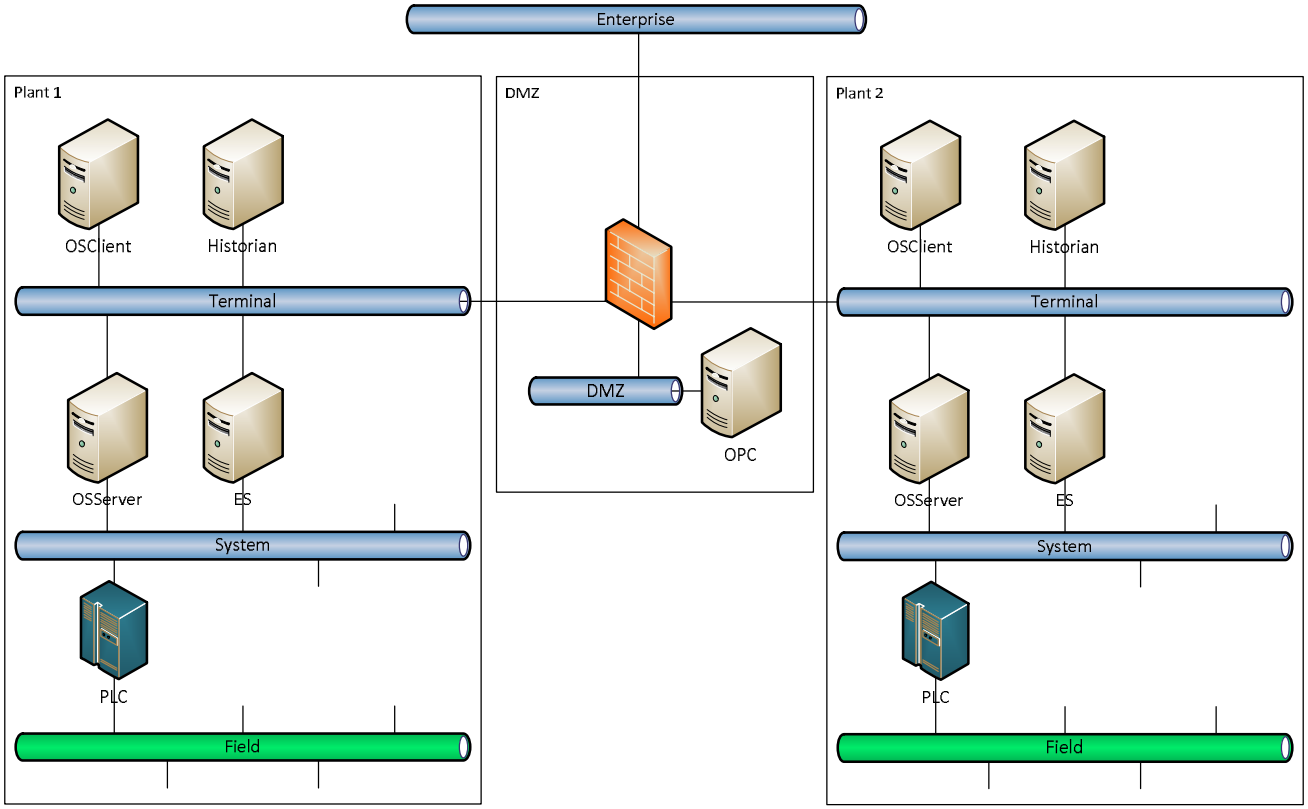
SIEMENS

Project deliverables

While the security posture check we assess your current state of security and after the check you will receive a report based on the tool with:

- Scope description
- Summary of the security gap check
- Result of the IEC62443 Tool
  - Graphical Overview of the reached levels
- Description of the findings
- Mitigation measures to increase the desired security level

IEC 62443 Assessment
Scope



IEC 62443 Assessment
Security Level

SIEMENS

TURVALLISUUDEN TASO (SL):

- Asteikolla 1-4

TASO 1: SL1 SL2 SL3 SL4

- *" Estetään sattumanvaraisia ja tahattomia tietoturvauhkia"*

ESIMERKKITULKINTOJA:

- *Työntekijät vahingossa aiheuttaa tuotantokatkoksen johtuen puutteellisestaperehdytyksestä*
- *Järjestelmiä avoimena intenetissä ja yleinen skannauspalvelu aiheuttaa katkoksen*

TASO 2: SL1 SL2 SL3 SL4

- *"Estetään tietoturvauhkia, joissa käytetään yksinkertaisia keinoja ja yleispäteviä taitoja. Hyökkääjä on aktiivinen ja omaa kohtalaiset resurssit ja matalan motivaation"*

ESIMERKKITULKINTOJA:

- *"Script kiddie"*
- *Suuttunut entinen työntekijä*

IEC 62443 Assessment
Security Level

SIEMENS

TURVALLISUUDEN TASO (SL):

- Asteikolla 1-4

TASO 3: SL1 SL2 **SL3** SL4

- *”Estetään tietoturvauhkia, joissa käytetään kehittyneitä keinoja ja teollisuusautomaation tuntemusta edellyttäviä erityistaitoja. Hyökkääjä on aktiivinen ja omaa kohtalaiset resurssit ja kohtalaisen motivaation”*

ESIMERKKITULKINTOJA:

- *Aktivistiryhmittymä*

TASO 4: SL1 SL2 SL3 **SL4**

- *”Estetään tietoturvauhkia, joissa käytetään kehittyneitä keinoja ja teollisuusautomaation tuntemusta edellyttäviä erityistaitoja. Hyökkääjä on aktiivinen ja omaa kattavat resurssit ja korkean motivaation”*

ESIMERKKITULKINTOJA:

- *Valtiollinen taho*

IEC 62443 Assessment
Stakeholders

SIEMENS

Project roles and responsibilities

During the assessment, the assessment team needs to carry out the interview with site personnel from different areas:

- Site management
- Site IT staff
- Production responsible persons for the different areas in scope of the assessment
- Maintenance staff
- Production planning staff
- Other stakeholders

IEC 62443 Assessment
Methodology III

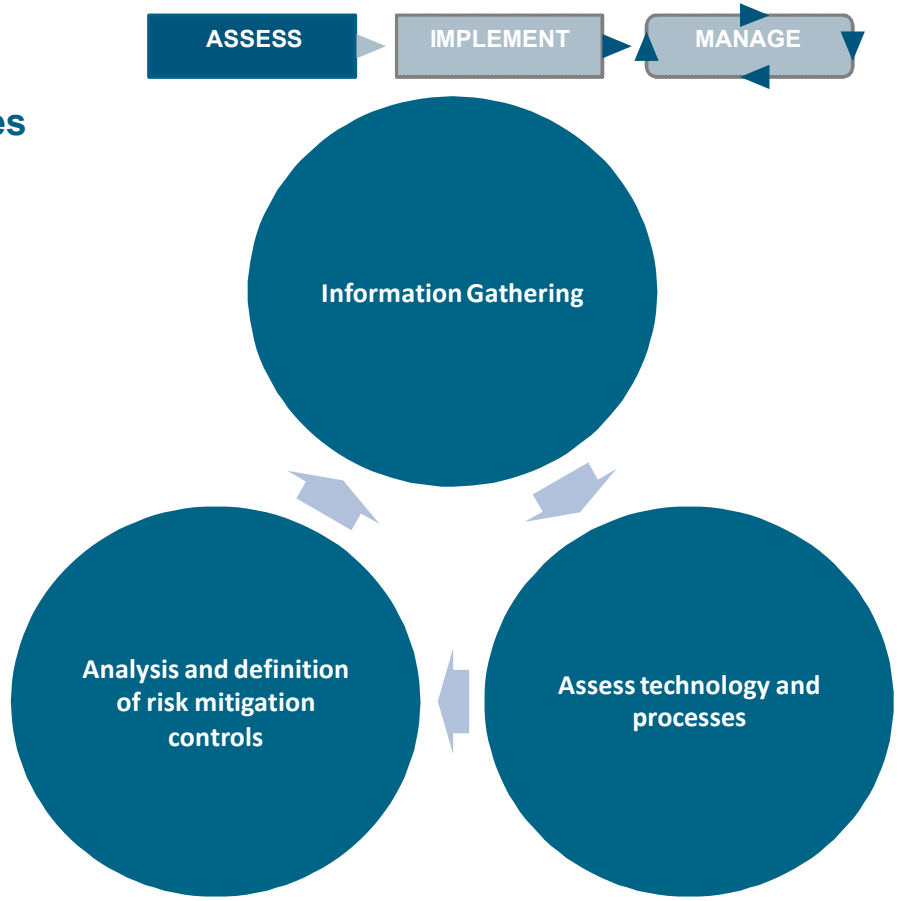
SIEMENS

Phased project approach based on IEC 62443, International best practices and our experience in several engagements conducted at many different types of facilities worldwide

Phase I: Kick-Off and Information Gathering*

* The scope of the assessment will be defined and agreed before project start

- The assessment project leader from the customer will provide a predefined list of documentation to be reviewed and analyzed by the assessment team, including:
  - Network overview
  - Network devices configuration
  - System security parameters (e.g. Hardening Measures)
  - Process flow diagrams (like input to output of product)
  - Security related policies and guidelines
  - If available, previous security audits or analysis reports
- **Project Kick-Off Meeting** (via Live Meeting or Conference Call)



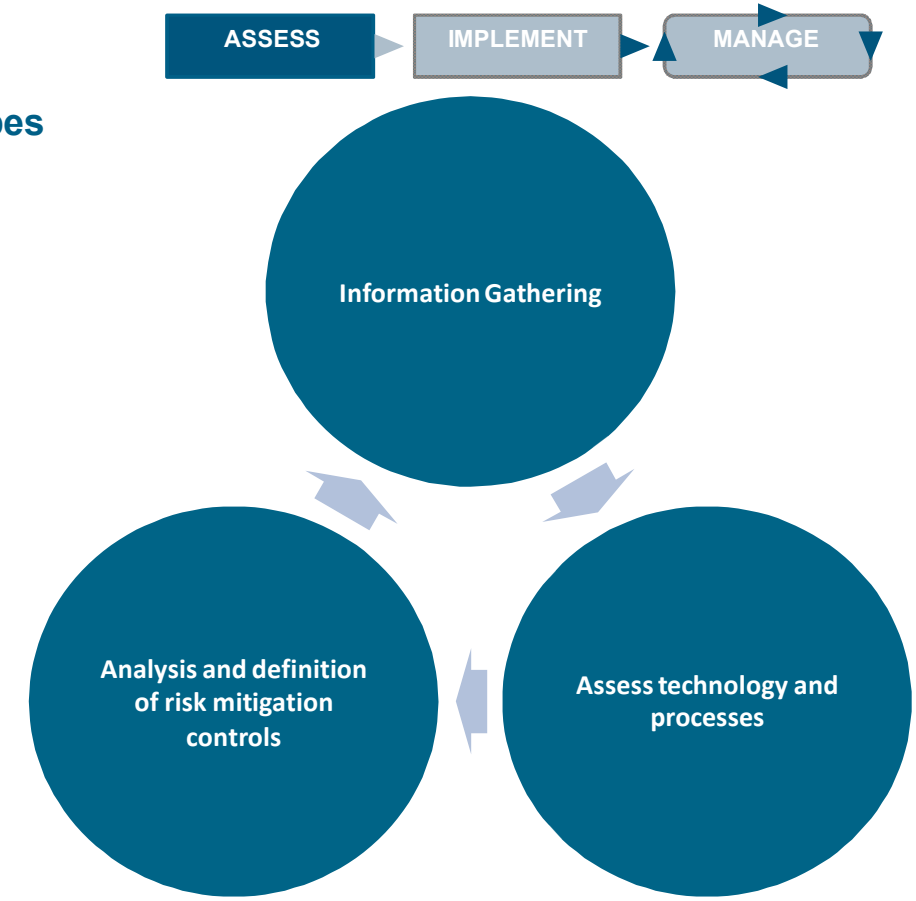
IEC 62443 Assessment
Methodology IV

SIEMENS

Phased project approach based on IEC 62443, International best practices and our experience in several engagements conducted at many different types of facilities worldwide

Phase II: On-site Assessment and Analysis

- **Interviews with stakeholders** to:
  - Assess the defined scope with IEC62443 based tool
  - Learn about existing protection mechanisms.
  - Learn about system criticality and threat likelihood.
- **Site visit and survey**



IEC 62443 Assessment
Methodology VII

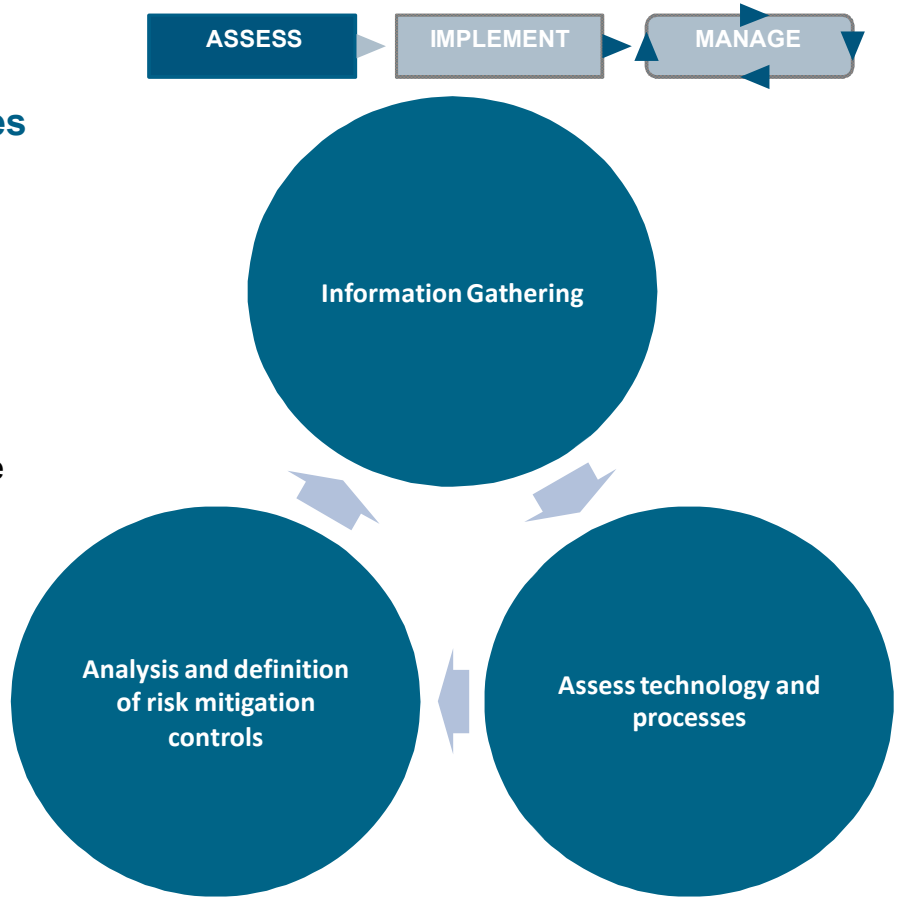
SIEMENS

Phased project approach based on IEC 62443, International best practices and our experience in several engagements conducted at many different types of facilities worldwide

Phase III: Report and mitigation suggestions

- **Including**:
  - Report based on IEC62443 tool
  - Suggestions to increase the Security level to the defined scope

- **Short Virtual Meeting (e.g. Livemeeting or similar) about the mitigations and defining next steps**

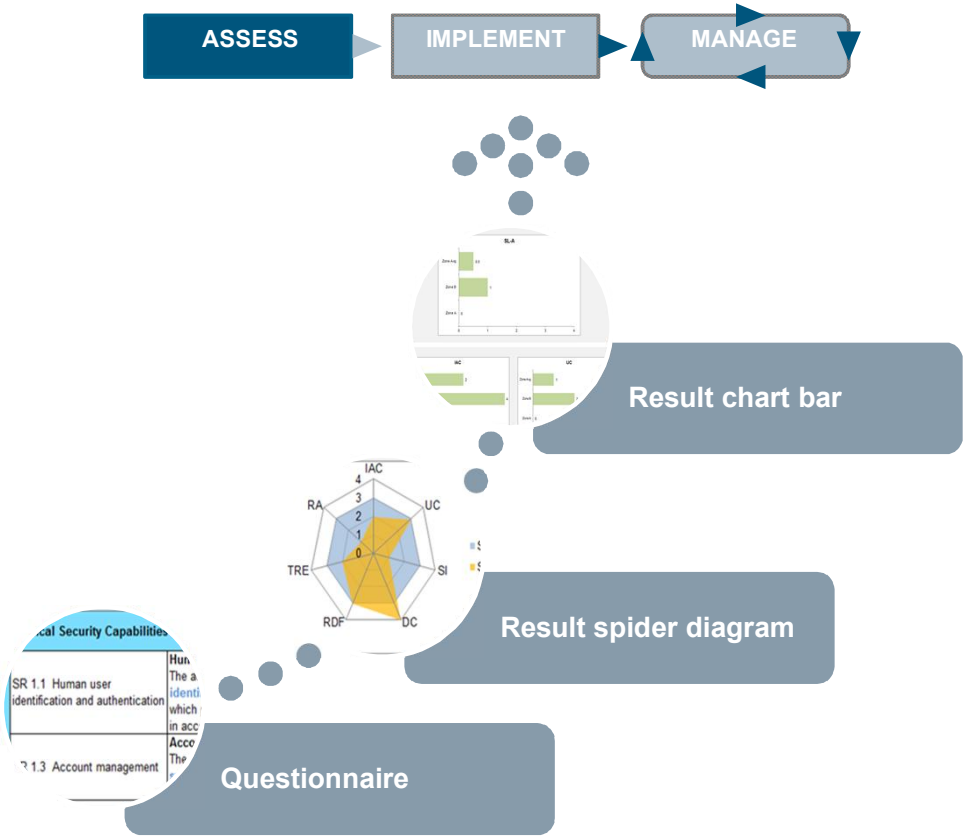


IEC 62443 Assessment
Methodology V

SIEMENS

Phased project approach based on IEC 62443-3-3 tool with following topics

- **FR 1 Identification and Access Control**
- **FR 2 Use Control**
- **FR 3 System Integrity**
- **FR 4 Data Confidentiality**
- **FR 5 Restrict Data Flow**
- **FR 6 Timely Response to Events**
- **FR 7 Resource Availability**

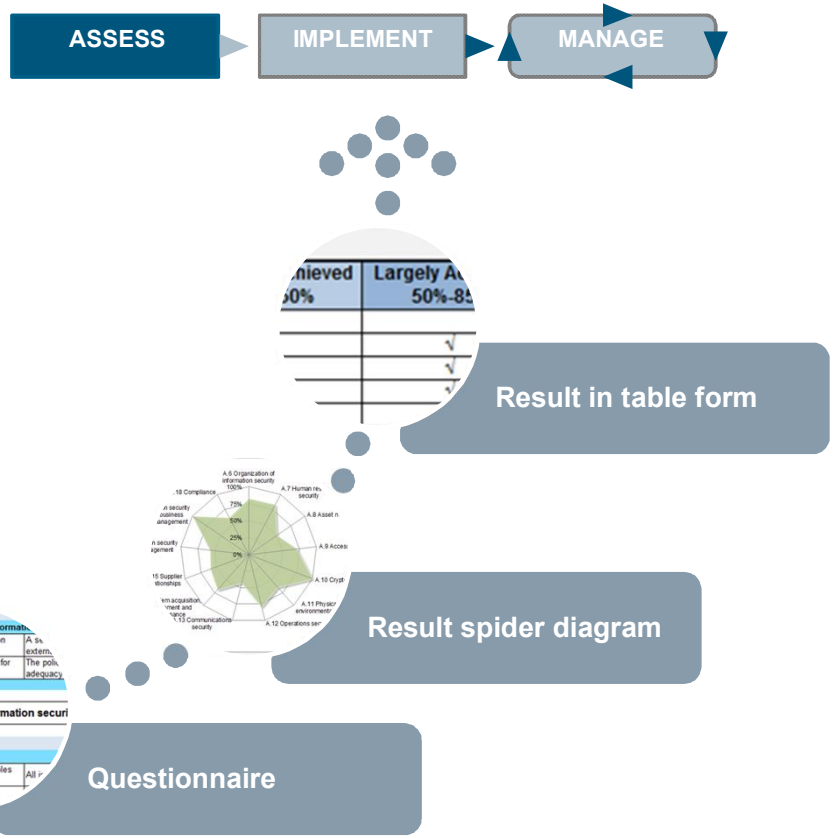


IEC 62443 Assessment
Methodology VI

SIEMENS

Phased project approach based on IEC 62443-2-1 tool with following topics

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

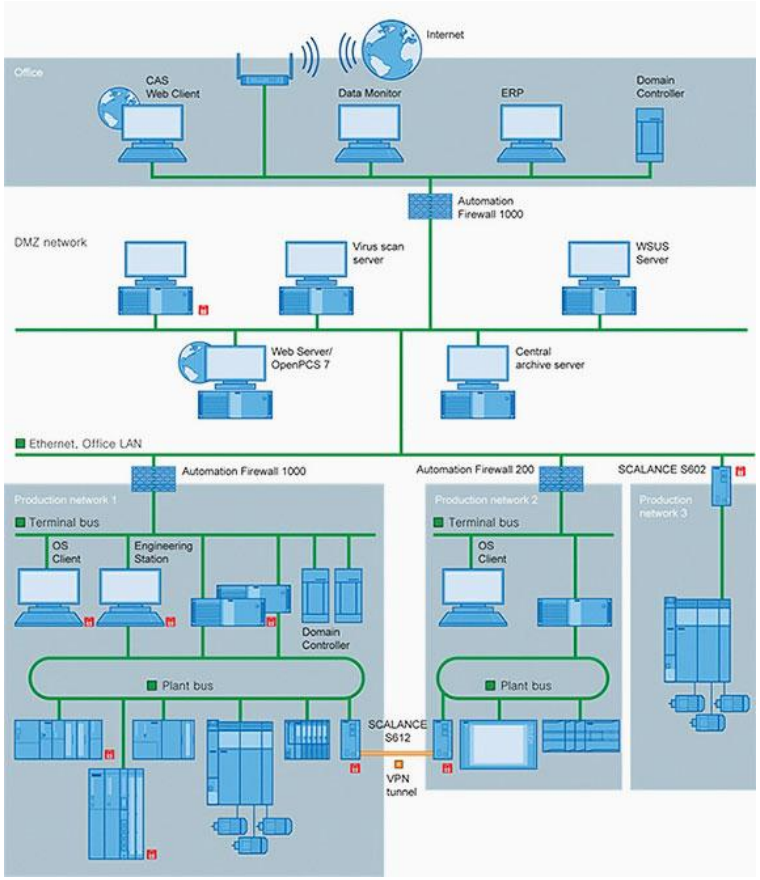


IEC62443 assesment
Practical example 1

SIEMENS

SR 5.1 – Network segmentation

The control system shall provide the capability to **logically** segment control system networks from non-control system networks and to **logically** segment critical control system networks from other control system networks.



IEC

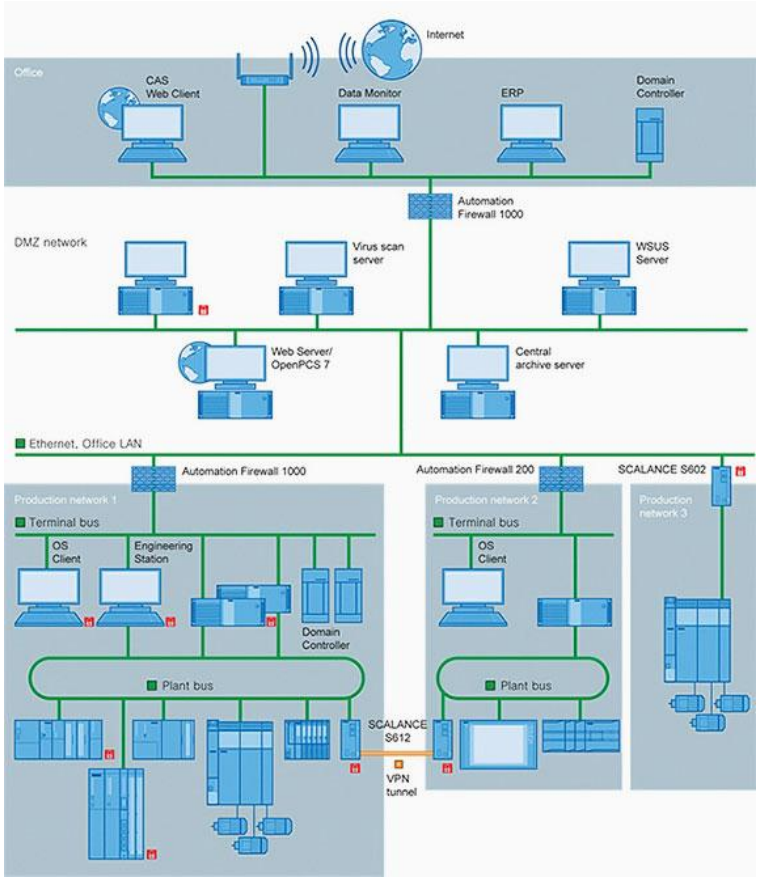
SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 1

SIEMENS

SR 5.1 RE 1 – Physical network segmentation

The control system shall provide the capability to **physically** segment control system networks from non-control system networks and to **physically** segment critical control system networks from non-critical control system networks.



IEC

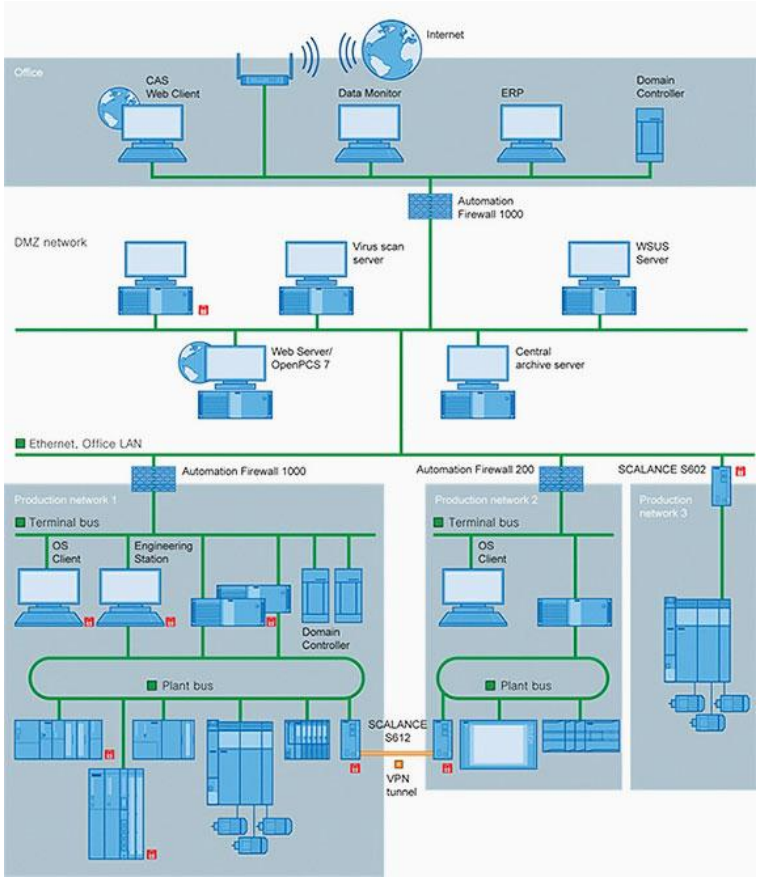
SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 1

SIEMENS

SR 5.1 RE 2 – Independence from non-control system networks

The control system shall have the capability to **provide network services** to control system networks, critical or otherwise, **without a connection to non-control** system networks.



IEC

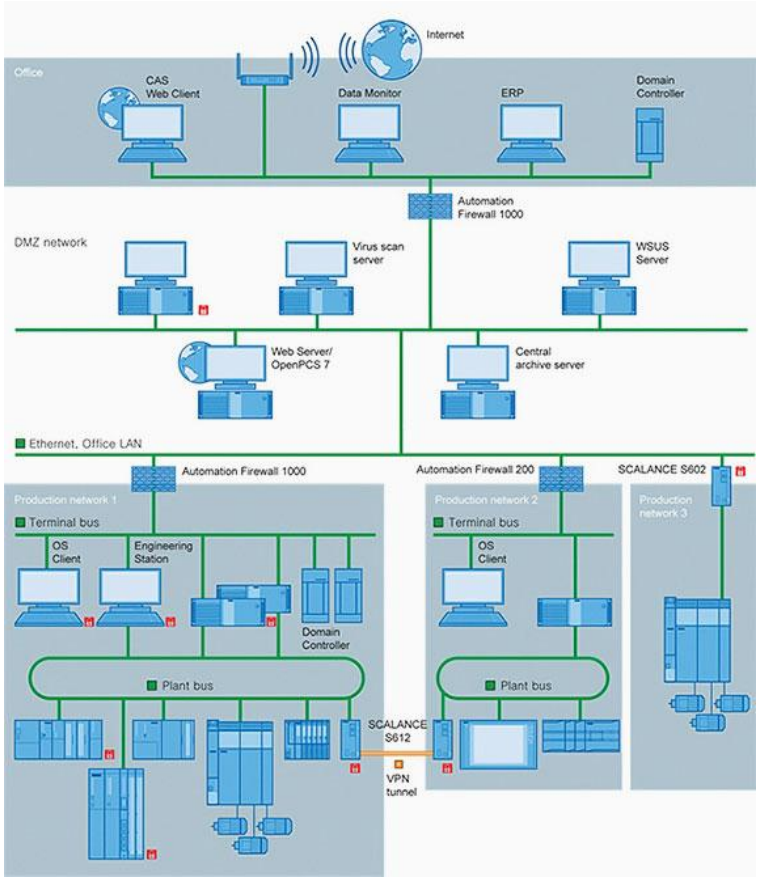
SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 1

SIEMENS

SR 5.1 RE 3 – Logical and physical isolation of critical networks

The control system shall provide the capability to **logically** and **physically isolate** critical control system networks from non-critical control system networks.



IEC

SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 2

SIEMENS

SR 7.3 – Control system backup

The **identity and location of critical files** and the ability to **conduct backups of user-level and system-level** information (including system state information) shall be supported by the control system without affecting normal plant operations.

IEC

SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 2

SIEMENS

SL2

SR 7.3 RE 1 – Backup verification

The control system shall provide the capability to **verify** the **reliability** of backup mechanisms.

IEC

SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 2

SIEMENS

SL3

SR 7.3 RE 2 – Backup automation

The control system shall provide the capability to **automate the backup function** based on a configurable frequency.

IEC

SL1 SL2 SL3 SL4

IEC62443 assesment
Practical example 3

SIEMENS

12.5.1 Change control procedures

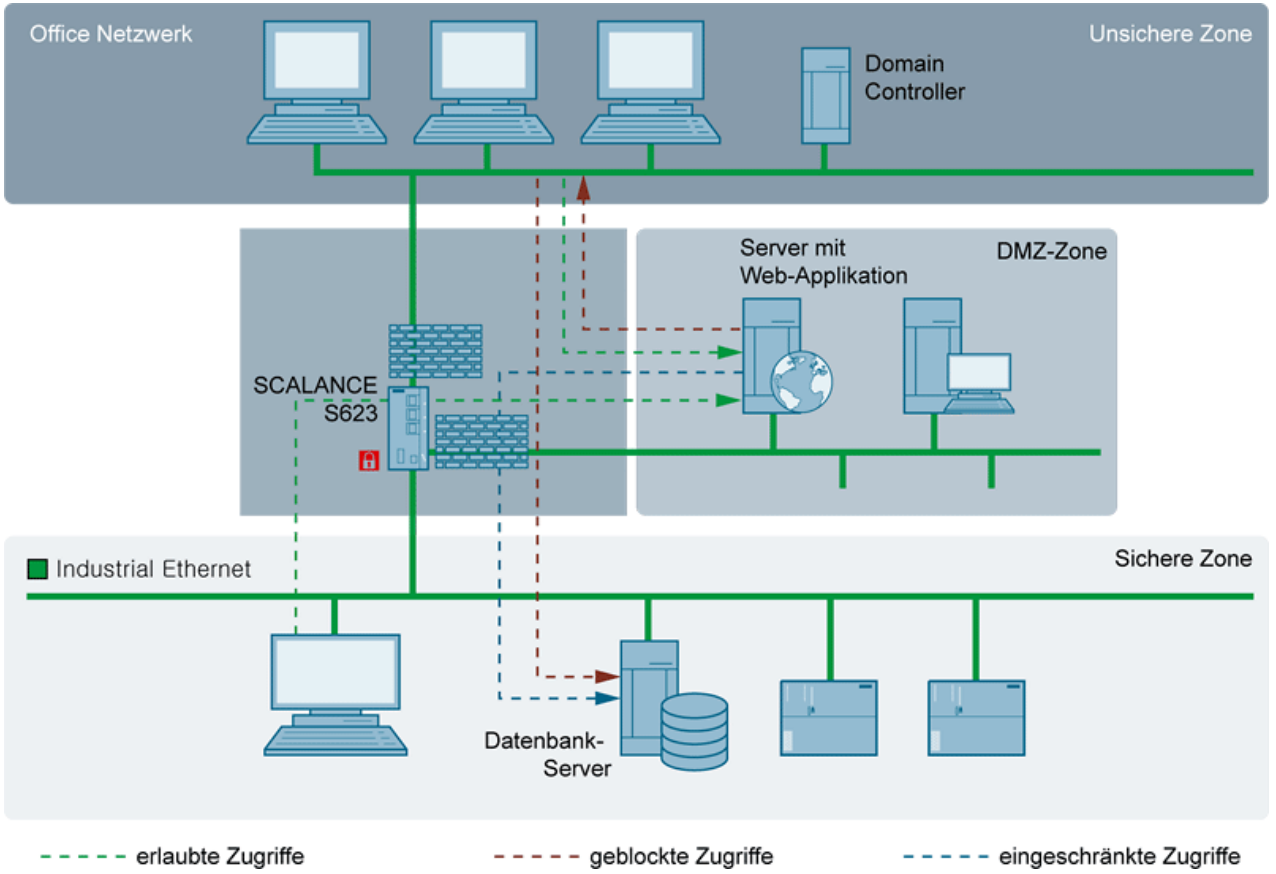
The implementation of changes shall be controlled by the use of formal change control procedures. A change management system for the IACS environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest.

IEC62443 assesment
Practical example 4

SIEMENS

Firewall

- Determination of needed data flow
- Configuration / Implementation
- Monitoring
- Responsibility
- Rule management
- Device management



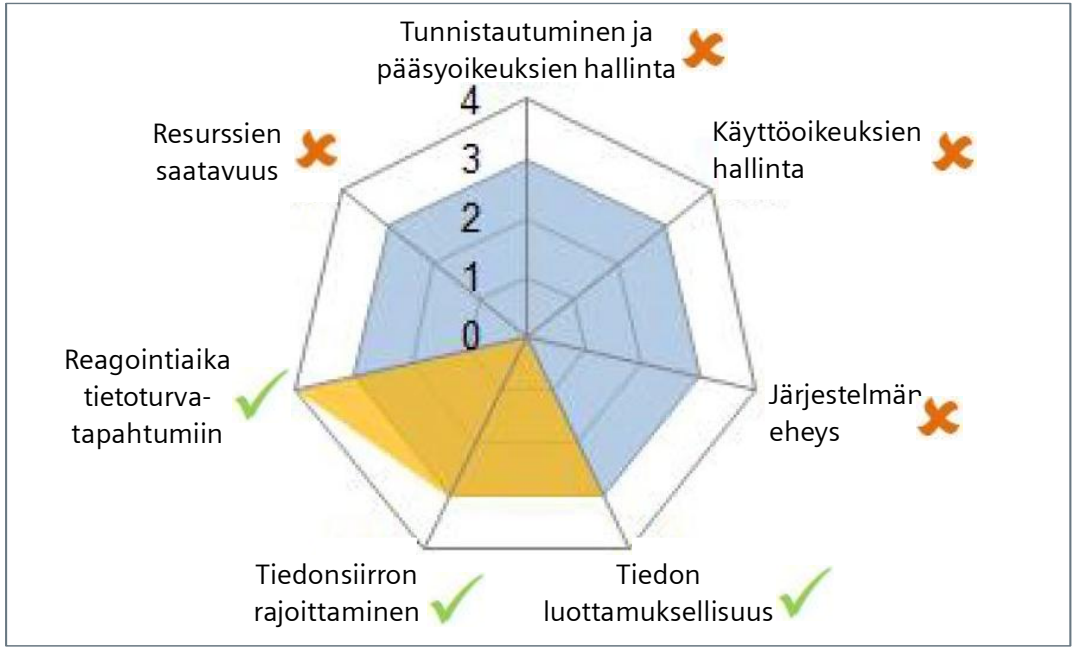
IEC62443 assesment
Tekninen osa (esimerkki)

SIEMENS

OLENNAISIMMAT PUUTTEET TAVOITETASOSTA:

- Puutteellinen ohjausjärjestelmän käyttöoikeuksien ja salasanojen hallinta
- Toimittajan VPN etäyhteyttä ei monitoroida
- Puutteellinen palomuuriprotokollien hallinta
- Puutteellinen USB tikkujen käytön hallinta
- Suoja haittaohjelmistoja (Malware) vastaan puuttuu
- Keskitetty laitelokien hallinta puuttuu
- Ohjausjärjestelmän turvaominaisuuksien dokumentaatio puuttuu
- Ohjausjärjestelmän varmuuskopioita ei testata tai skannata haittaohjelmistojen varalta

TEKNINEN TIETOTURVAKARTOITUS:



LEGEND:

IEC62443 assesment
Hallinnollinen osa (esimerkki)

SIEMENS

OLENNAISIMMAT PUUTTEET TAVOITETASOSTA:

Operointi:

- Operoinnin keskitetty monitorointi ja hallinta puuttuu
- Keskitetty lokienhallinta puuttuu

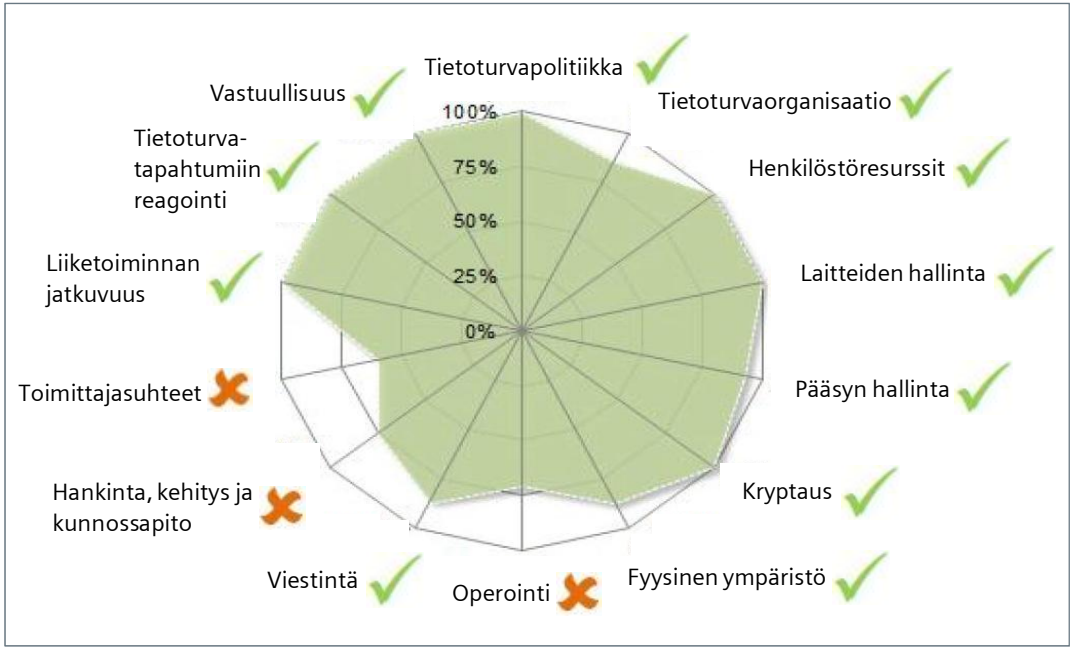
Hankinta, kehitys ja kunnossapito:

- Ohjausjärjestelmän muutostenhallinta puuttuu
- Ohjausjärjestelmän kehitysympäristö ei täytä tietoturvavaatimuksia
- Ohjausjärjestelmän turvaominaisuuksille ei ole vaatimusmäärittelyä

Toimittajasuhteet:

- Toimittajille ei ole tietoturvavaatimuksia / -ohjeistusta
- Toimittajia ei ole ohjeistettu riskien- / haavoittuvuuksien raportointiin

HALLINNOLLINEN TIETOTURVAKARTOITUS:

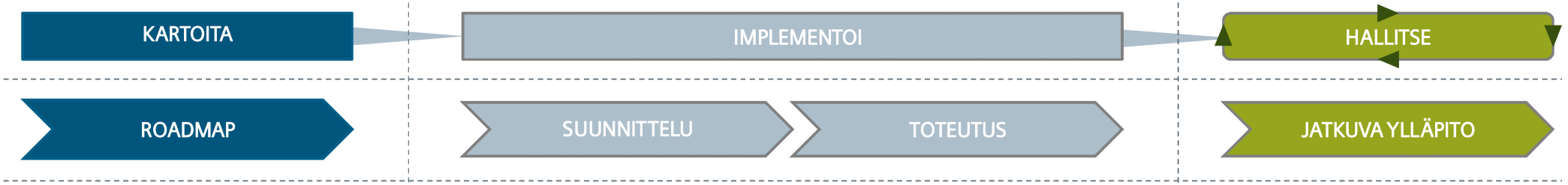


LEGEND:

Tavoitetaso saavutettu	Puutteita havaittu

IEC62443 assesment
Toimenpidesuositukset ja roadmap

SIEMENS



- Pidetään workshop, jossa määritellään tarkemmin tietoturvan implementointi-toimenpiteet
- Määritellään karkea aikataulu
- Esitellään kartoitus yritysjohdolle
- Johdon päätös

- Yksityiskohtainen implementointisuunnitelma kartoituksen mukaan
- Mikäli tarpeen, rakennetaan testiympäristö konseptin validointia varten
- Hallitun palvelun ja ylläpidon alustavat toimenpiteet
- Teknologian implementointi ja käyttöönotto
- Laitoksen tietoturvadokumentaation päivittäminen vastaamaan uutta konseptia
- Käyttäjäkoulutus
- Loppukäyttäjän hyväksyntä
- Tarvittavan tiedon ja dokumentaation luovuttaminen palvelukeskukselle ylläpitoa ja monitorointia varten

- Jatkuva tietoturvan monitorointi
- Hallittu palveluratkaisu
- Asiakaskohtaiset hälytykset
- Säännöllinen raportointi
- Syklinen kyberturvakonseptin tehokkuuden uudelleen arviointi

Yhteydenotot

Jyrki Keinänen

SIEMENS OSAKEYHTIÖ
Plant Security Services

Tarvonsalmenkatu 19
FI-02600 Espoo

E-Mail: jyrki.keinanen@siemens.com

Puh.: +358 50 576 1125

siemens.com/plant-security-services