Standardisarja IEC 62443

Teollisuuden tietoliikenneverkot
Verkkojen ja järjestelmien tietoturvallisuus

Matti Sundquist, Sundcon Oy

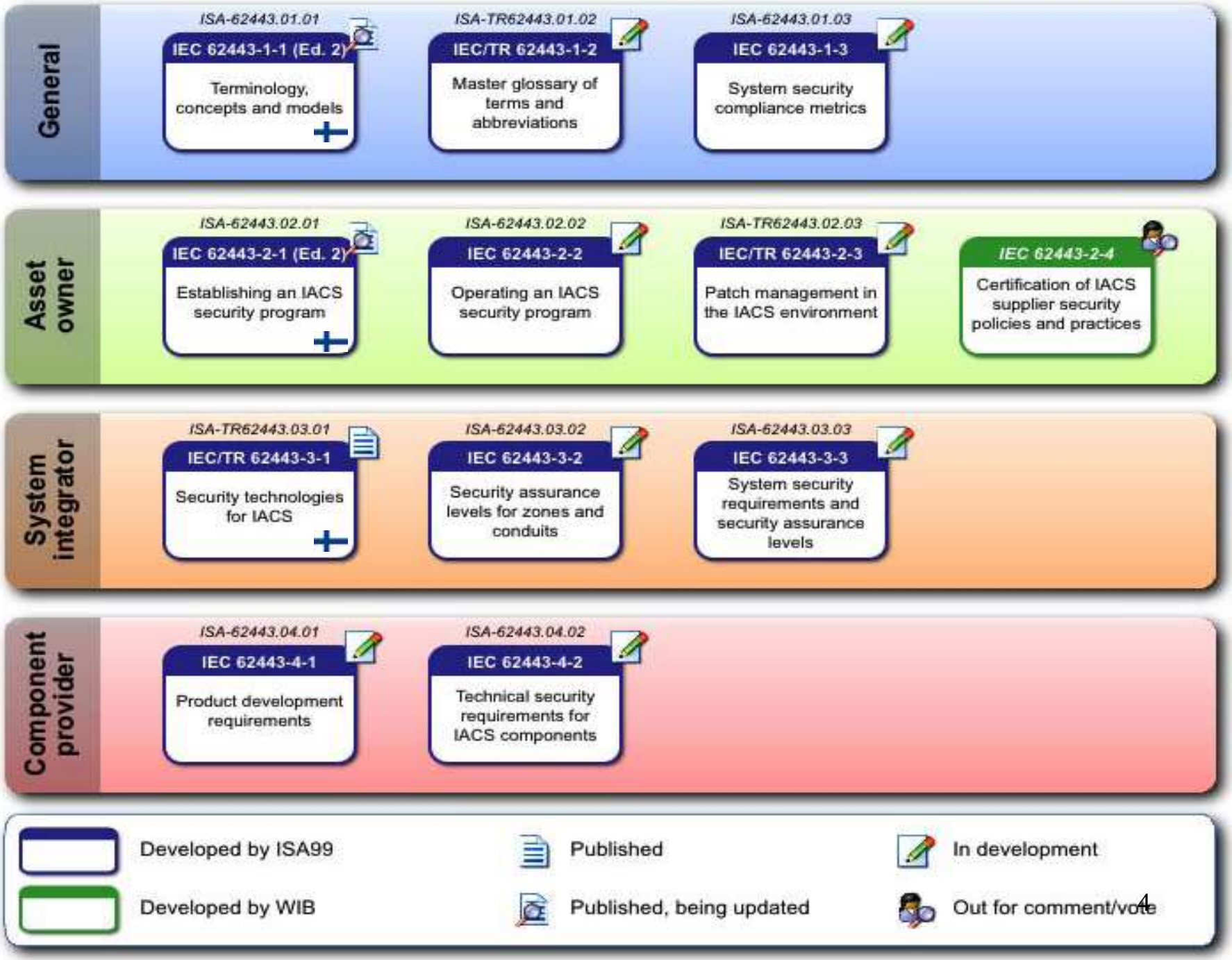
Jukka Alve, SESKO ry

ASAFin tietoturvaseminaari 27.1.2004

Automaatioseuran julkaisu: Teollisuusautomaation tietoturva – verkottumisen riskit, CERT-FI:
http://www.cert.fi/attachments/cip/5na1SblCp/SAS29_TeollisuusautomaationTietoturva.pdf

Teollisuusautomaation standardit

- Teollisuuden automaatio- ja ohjausjärjestelmien standardoinnista vastaa Seskon komitea SK 65 ”Teollisuusprosessien mittaus ja ohjaus (teollisuusautomaatio)”.
- SK 65 on IEC TC 65:n ja CENELEC TC 65:n vastinkomitea Suomessa.
- SK65 alaan kuuluvia standardeja on lähes 300 kappaletta
- Standardien hakemisen ja käytön helpottamiseksi on julkaistu verkkokirja teollisuusautomaation standardista (www.automaatioseura.fi).

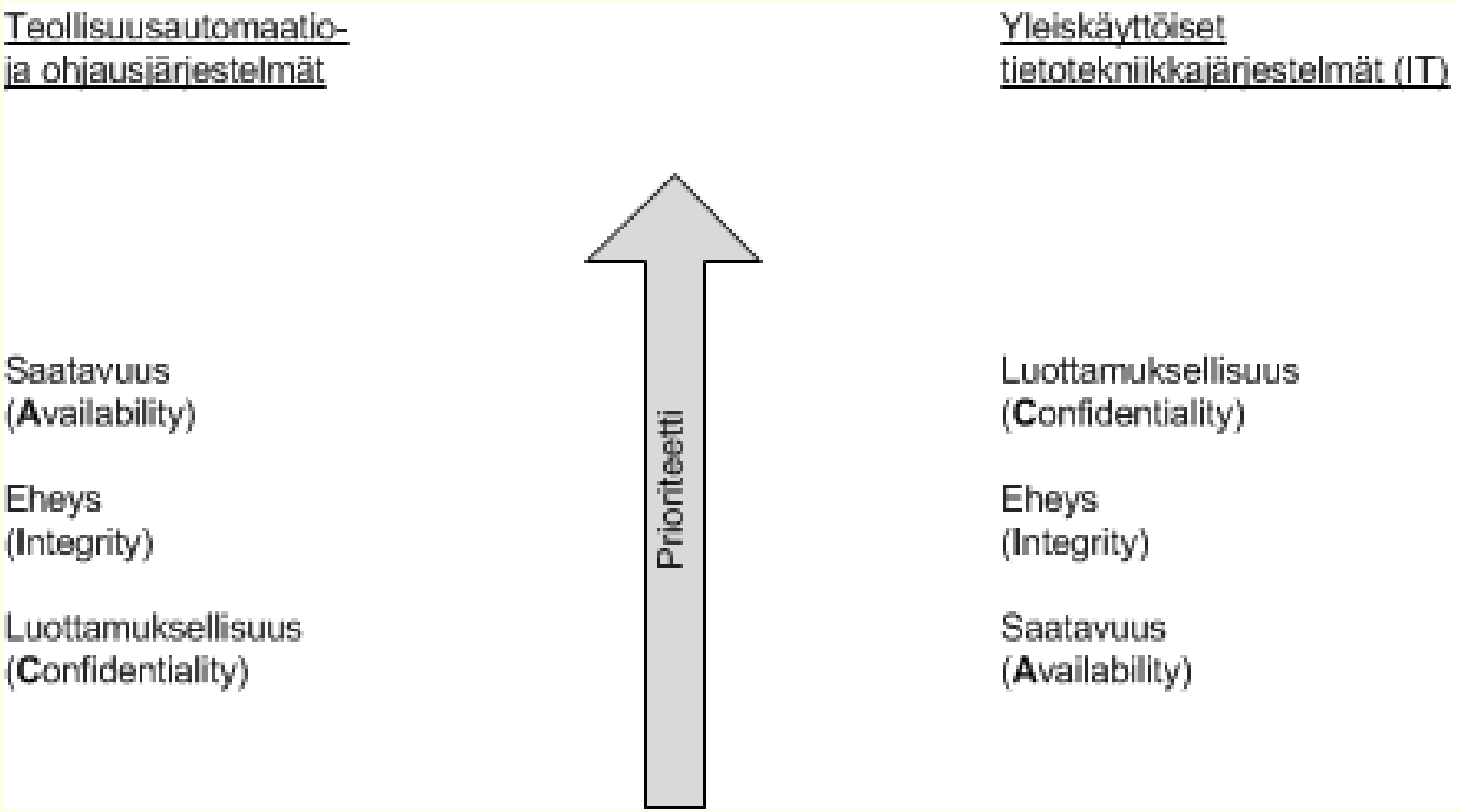

General
ISA-62443.01.01
IEC 62443-1-1 (Ed. 2)
Terminology, concepts and models
ISA-TR62443.01.02
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
ISA-62443.01.03
IEC 62443-1-3
System security compliance metrics
Asset owner
ISA-62443.02.01
IEC 62443-2-1 (Ed. 2)
Establishing an IACS security program
ISA-62443.02.02
IEC 62443-2-2
Operating an IACS security program
ISA-TR62443.02.03
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Certification of IACS supplier security policies and practices
System integrator
ISA-TR62443.03.01
IEC/TR 62443-3-1
Security technologies for IACS
ISA-62443.03.02
IEC 62443-3-2
Security assurance levels for zones and conduits
ISA-62443.03.03
IEC 62443-3-3
System security requirements and security assurance levels
Component provider
ISA-62443.04.01
IEC 62443-4-1
Product development requirements
ISA-62443.04.02
IEC 62443-4-2
Technical security requirements for IACS components
Developed by ISA99
Developed by WIB
Published
Published, being updated
In development
Out for comment/vote

Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus

Suomi – englanti versiot:

- IEC/TS 62443-1-1:fi
  - Osa 1-1: Terminologia, käsitteet ja mallit
- IEC 62443-2-1:fi
  - Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten
- IEC/TR 62443-3-1:fi
  - Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille

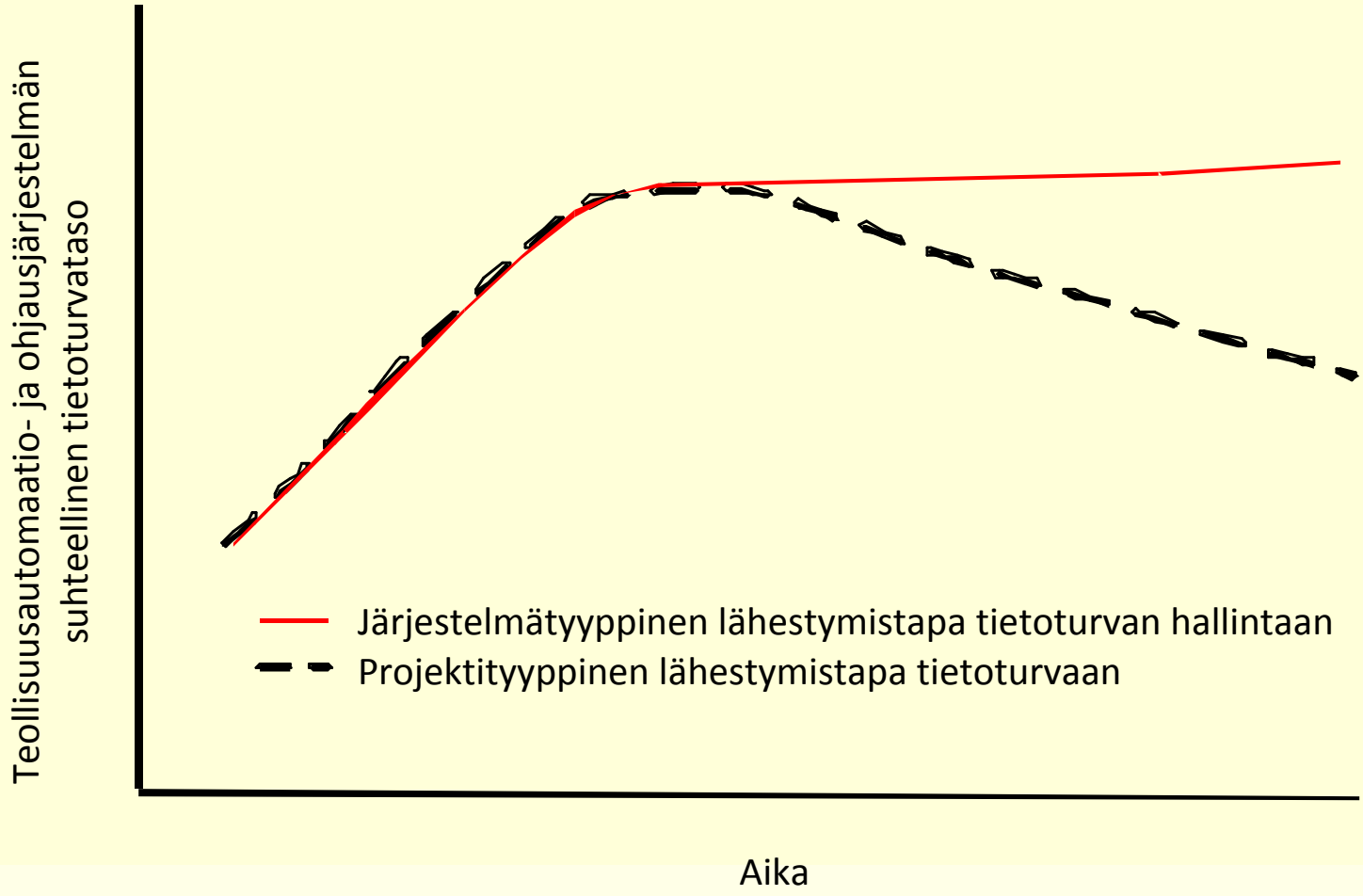
Tavoitteiden käänteinen tärkeysjärjestys



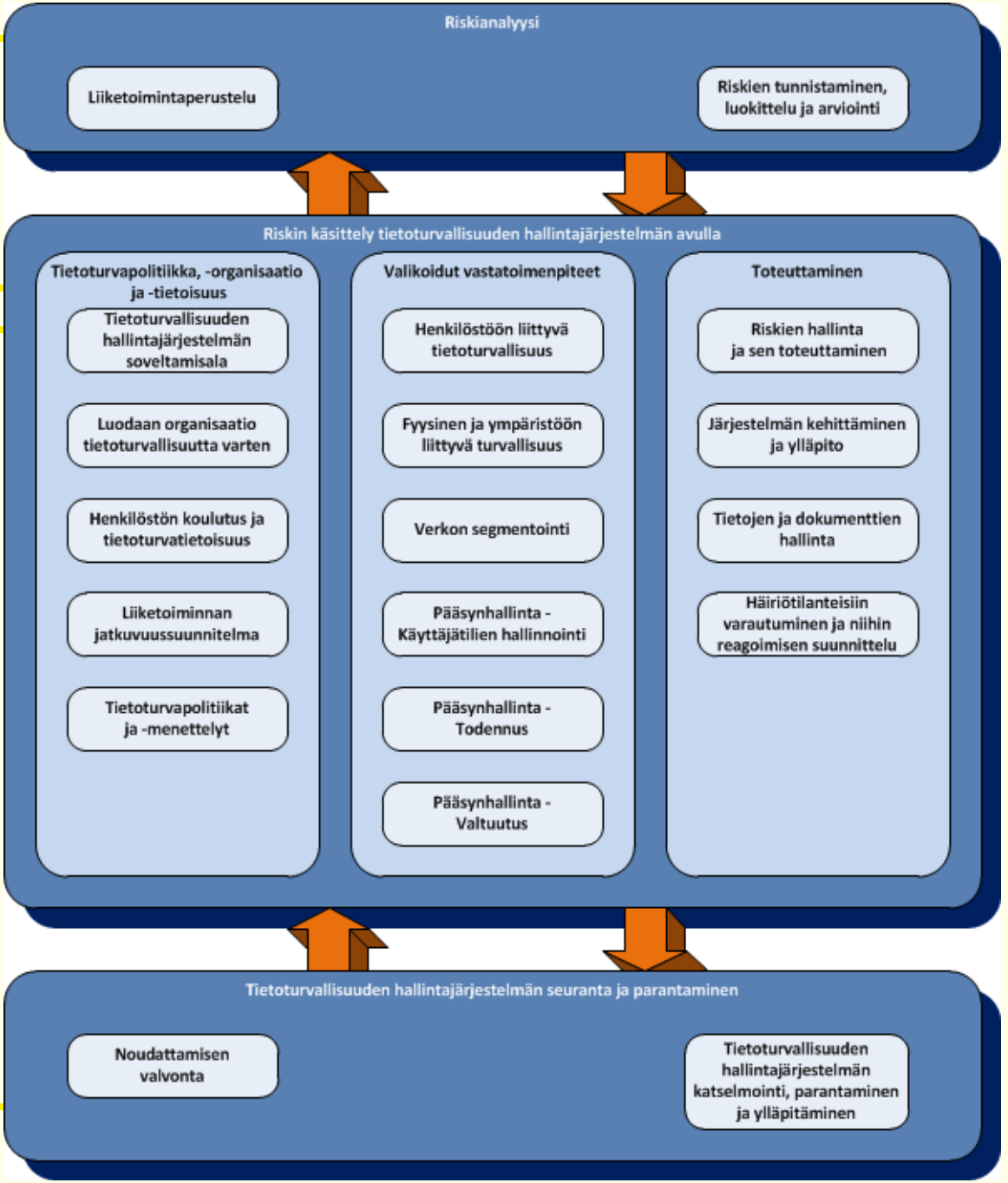
Teollisuusautomaation vs. tietotekniikan tietoturvallisuus

- Useita tietotekniikassa (IT) käytettyjä menetelmiä ei voida sellaisenaan soveltaa teollisuuden automaatio- ja ohjausjärjestelmiin (IACS)
- Tietoturvallisuuden tavoitteet ovat osittain käänteisiä teollisuuden automaatio- ja ohjausjärjestelmiin, esim.:
  - saatavuus vs. luottamuksellisuus
  - mahdolliset terveys-, turvallisuus- ja ympäristövaikutukset.
- IACS-tietoturvastandardissa IEC 62443 viitataan IT-tietoturvastandardiin ISO/IEC 27001
  - standardien vastaavuudet esitetään osan 2-2 liitteessä.

Tietoturva on jatkuvasti ylläpidettävä prosessi, ei projekti



Tietoturvallisuuden hallintajärjestelmän elementit



IEC/TS 62443-1-1:fi

Terminologia	Käsitteet	Mallit
• Termit • Määritelmät • Lyhenteet	• Tietoturvatavoitteet • Perusvaatimukset • Syvyyssuuntainen puolustus • Tietoturva-asiayhteys • Uhkien ja riskien arvioinnit • Tietoturvallisuusohjelman kypsyys • Politiikat • Tietoturvavyöhykkeet • Tietoväylät • Tietoturvatasot • Tietoturvatason elinkaari	• Referenssimallit • Suojattavien kohteiden mallit • Referenssiarkkitehtuuri • Vyöhyke- ja tietoväylämalli • Mallien väliset suhteet

IEC 62443-2-1:fi

Riskianalyysi	Riskin käsittely tietoturvallisuuden hallintajärjestelmän avulla	Tietoturvallisuuden hallintajärjestelmän seuranta ja parantaminen
• Liiketoimintaperustelu • Riskien tunnistaminen, luokittelu ja arviointi	• Tietoturvapolitiikka, -organisaatio ja -tietoisuus • Valikoidut vastatoimenpiteet • Toteuttaminen	• Noudattamisen valvonta • Tietoturvallisuuden hallintajärjestelmän katselmointi, parantaminen ja ylläpitäminen
Liite A (opastava) Neuvoja tietoturvallisuuden hallintajärjestelmän elementtien kehittämistä varten Liite B (opastava) Tietoturvallisuuden hallintajärjestelmän kehittämisprosessi Liite C (opastava) Vaatimusten rinnastaminen standardin ISO/IEC 27001 vaatimuksiin		

IEC/TR 62443-3-1:fi (1/2)

Todennus- ja valtuutusteknologiat	Suodatuksen / estämisen / pääsyn hallinan teknologiat	Salausteknologiat ja tietojen kelpuutus
• Roolipohjaiset valtuutustyökalut • Salasanaan perustuva todennus • Haaste-vaste-todennus • Todennus toimikortilla • Biometrinen todennus • Sijaintiin perustuva todennus • Salasanojen jakelun ja hallinnan teknologiat • Laitteesta laitteeseen -todennus	• Verkon palomuurit • Käyttöjärjestelmään asennetut palomuurit • Virtuaaliverkot	• Symmetriseen (salaiseen) avaimeen perustuva salaus • Julkiseen avaimeen perustuva salaus ja avaimen jakelu • VPN-verkot

IEC/TR 62443-3-1:fi (2/2)

Hallinta-, auditointi-, mittaus-, valvonta- ja havaitsemistyökalut	Teollisuusautomaatio- ja ohjausjärjestelmien tietokoneohjelmistot	Fyysinen tietoturvan valvonta
• Lokitietojen auditointivälineet • Virusten ja haittakoodien havaitsemisjärjestelmät • Tunkeutumisen havaitsemisjärjestelmät (IDS) • Haavoittuvuusskannerit • Tutkinta- ja analysointityökalut (FAT) • Isäntäkoneen hallinnan työkalut (HCM) • Ohjelmistojen automaattiset hallintatyökalut (ASM)	• Palvelimien ja työasemien käyttöjärjestelmät • Tosiaikaiset ja sulautetut käyttöjärjestelmät • Web-teknologiat	• Fyysinen suojaus • Henkilöstöön liittyvä tietoturva