



Toiminnallinen turvallisuus ja kyberturvallisuus osana koneturvallisuutta

Janne Peltonen, 13.11.2025, METSTA Turvallisen tekniikan seminaari, Tampere-talo

kiwa

Teemat

Koneiden ohjausjärjestelmien toiminnallinen turvallisuus uuden EU:n koneasetuksen mukaisesti

- Koneiden ja vastaavien tuotteiden on täytettävä asetetut olennaiset terveys- ja turvallisuusvaatimukset;
- Turvallisuuteen liittyvä ohjausjärjestelmä toteuttaa koneen turvallisen tilan saavuttamiseksi ja ylläpitämiseksi tarpeelliset vaaditut turvatoiminnot;
- Turvallisuuteen liittyvä ohjausjärjestelmä on tarkoitettu saavuttamaan yksin tai yhdessä muiden turvallisuuteen liittyvien järjestelmien tai ulkoisten riskien pienennyskeinojen kanssa riittävä riskien pienentäminen.

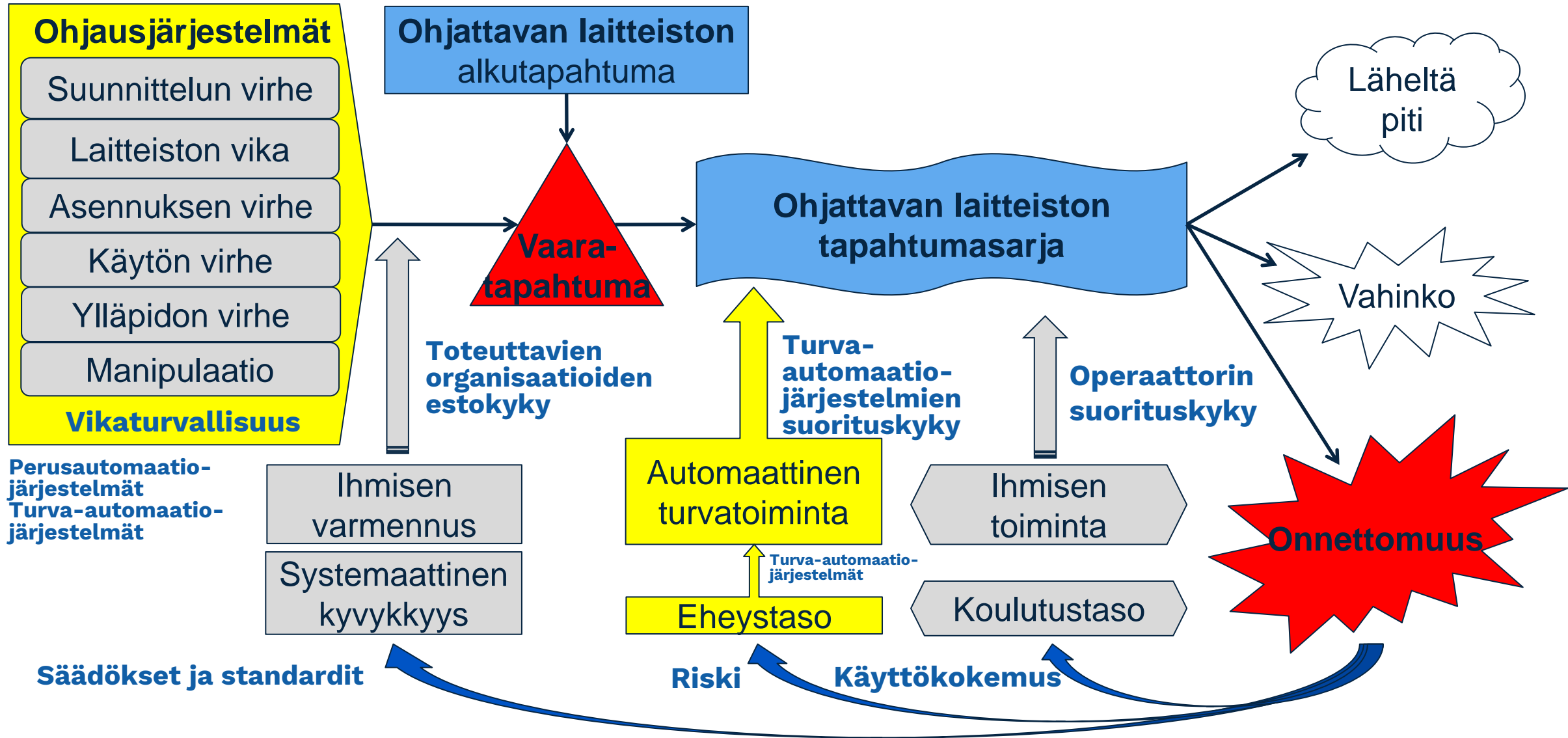
Koneiden ohjausjärjestelmien kyberturvallisuus uuden EU:n koneasetuksen mukaisesti

- Yhteys koneen riskinarviointiin;
- Standardien valinta ja vaatimukset.

Pohdintaa mahdollisista vaikutuksista

- *”Koska on hankittu ja otettu käyttöön epäluotettavia tietokoneteknologioita, kaikkien organisaatioiden olisi ryhdyttävä uudelaisiin ja aiemmin tarpeettomiin töihin, jotta tietokoneet pysyisivät pystyssä kaatumatta ja lukkiutumatta, eivätkä aiheuttaisi vahinkoa.”*

Mitä on toiminnallinen turvallisuus?



Perusteita

Koneiden turvallisuutta koskeva lainsäädäntö edellyttää ohjausjärjestelmiltä toiminnallista turvallisuutta:

- Pää tavoitteena toiminnallisessa turvallisuudessa on henkilön, yhteiskunnan ja ympäristön turvallisuus sekä taloudellisten vahinkojen minimointi.
- EU:n uusi koneasetus (EU) 2023/1230 edellyttää ohjausjärjestelmiltä turvallisuutta ja toimintavarmuutta.
- Turvallisuuteen liittyvä ohjausjärjestelmä (engl. safety-related control system, safety-related parts of the control system) on yksi keino lisätä koneen turvallisuutta.
- Ohjelmoitavaa turvallisuuteen liittyvää ohjausjärjestelmää ei laki velvoita, mutta suojaustoimenpiteet katsotaan usein helpoimmaksi toteuttaa ohjelmoitavalla nykytekniikalla.
- Toiminnallinen turvallisuus on määritelty toimialoista riippumattomassa kattostandardissa IEC 61508.
- Koneiden turvallisuuteen liittyviä ohjausjärjestelmiä koskeva EU:n alueella yhdenmukaistettu standardi on EN IEC 62061, joka on kattostandardin IEC 61508 perusteella laadittu sovellussektoristandardi.
- Koneiden turvallisuuteen liittyvien ohjausjärjestelmien osia koskeva EU:n alueella yhdenmukaistettu standardi on EN ISO 13849-1, joka viittaa kattostandardiin IEC 61508 lukuisissa kohdissa.

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveyst- ja turvallisuusvaatimukset

Ohjausjärjestelmän vaatimusten lisäykset alleviivattuna

1.2.1 Ohjausjärjestelmien turvallisuus ja toimintavarmuus

- Ohjausjärjestelmät on suunniteltava ja rakennettava sellaisiksi, että ne estävät vaaratilanteiden syntymisen.
- Ohjausjärjestelmät on suunniteltava ja rakennettava siten, että
 - a) ne kestävät, jos se on olosuhteiden ja riskien kannalta tarkoituksenmukaista, tarkoitetut käyttörasitukset sekä tarkoitetut ja tarkoittamattomat ulkoiset vaikutukset, mukaan lukien kolmansien osapuolten kohtuudella ennakoitavissa olevat pahantahtoiset yritykset, jotka voivat aiheuttaa vaaratilanteen;
 - b) ohjausjärjestelmän laitteisto- tai logiikkavika ei saa aiheuttaa vaaratilanteita;
 - c) virheet ohjausjärjestelmän logiikassa eivät saa aiheuttaa vaaratilanteita;
 - d) turvatoimintojen rajat on vahvistettava osana valmistajan suorittamaa riskinarviointia, ja koneen tai vastaavan tuotteen tai käyttäjien tekemiä muutoksia asetuksiin tai sääntöihin ei sallita, ei myöskään koneen tai vastaavan tuotteen oppimisvaiheen aikana, jos tällaiset muutokset voisivat aiheuttaa vaaratilanteita;
 - e) kohtuudella ennakoitavissa olevat inhimilliset erehdykset käytön aikana eivät saa aiheuttaa vaaratilanteita;

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveyst- ja turvallisuusvaatimukset

Ohjausjärjestelmän vaatimusten lisäykset alleviivattuna

1.2.1 Ohjausjärjestelmien turvallisuus ja toimintavarmuus

- (jatkoa edelliseltä kalvolta)
- f) koneen tai vastaavan tuotteen markkinoille saattamisen tai käyttöönoton jälkeen ladattujen turvallisuus ohjelmiston versioiden sekä toimenpiteen yhteydessä tuotettavan datan jäljitysloki on käytettävissä viiden vuoden ajan tällaisen latauksen jälkeen yksinomaan sen osoittamiseksi, että kone tai vastaava tuote on tämän liitteen mukainen, siinä tapauksessa, että toimivaltainen kansallinen viranomainen esittää perustellun pyynnön tämän tiedon saamiseksi.

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveys- ja turvallisuusvaatimukset

Ohjausjärjestelmän vaatimusten lisäykset alleviivattuna

1.2.1 Ohjausjärjestelmien turvallisuus ja toimintavarmuus

- (jatkoa edelliseltä kalvolta)
- Sellaisten koneiden tai vastaavien tuotteiden ohjausjärjestelmät, joissa on tarkoituksella täysin tai osittain itsekehittyvä käyttäytyminen tai logiikka ja jotka on suunniteltu toimimaan erilaisilla autonomian tasoilla, on suunniteltava ja rakennettava sellaisiksi, että
 - a) kone tai vastaava tuote ei saa ohjausjärjestelmän vuoksi suorittaa toimia, jotka ylittävät sille määritellyn tehtävän ja liikkumistilan;
 - b) datan tallentaminen turvallisuuteen liittyvästä päätöksentekoprosessista ohjelmistopohjaisissa turvallisuusjärjestelmissä, jotka varmistavat turvatoiminnon, turvakomponentit mukaan luettuina, sen jälkeen, kun kone tai vastaava tuote on saatettu markkinoille tai otettu käyttöön, on kytketty päälle ja tällainen data säilytetään yhden vuoden ajan sen keräämisestä yksinomaan sen osoittamiseksi, että kone tai vastaava tuote on tämän liitteen mukainen, siinä tapauksessa, että toimivaltainen kansallinen viranomainen esittää perustellun pyynnön tämän tiedon saamiseksi;
 - c) koneen tai vastaavan tuotteen toimintaa on voitava korjata milloin tahansa, jotta se pysyy luontaisesti turvallisena.

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveyst- ja turvallisuusvaatimukset Ohjausjärjestelmän vaatimusten lisäykset alleviivattuna

1.2.1 Ohjausjärjestelmien turvallisuus ja toimintavarmuus

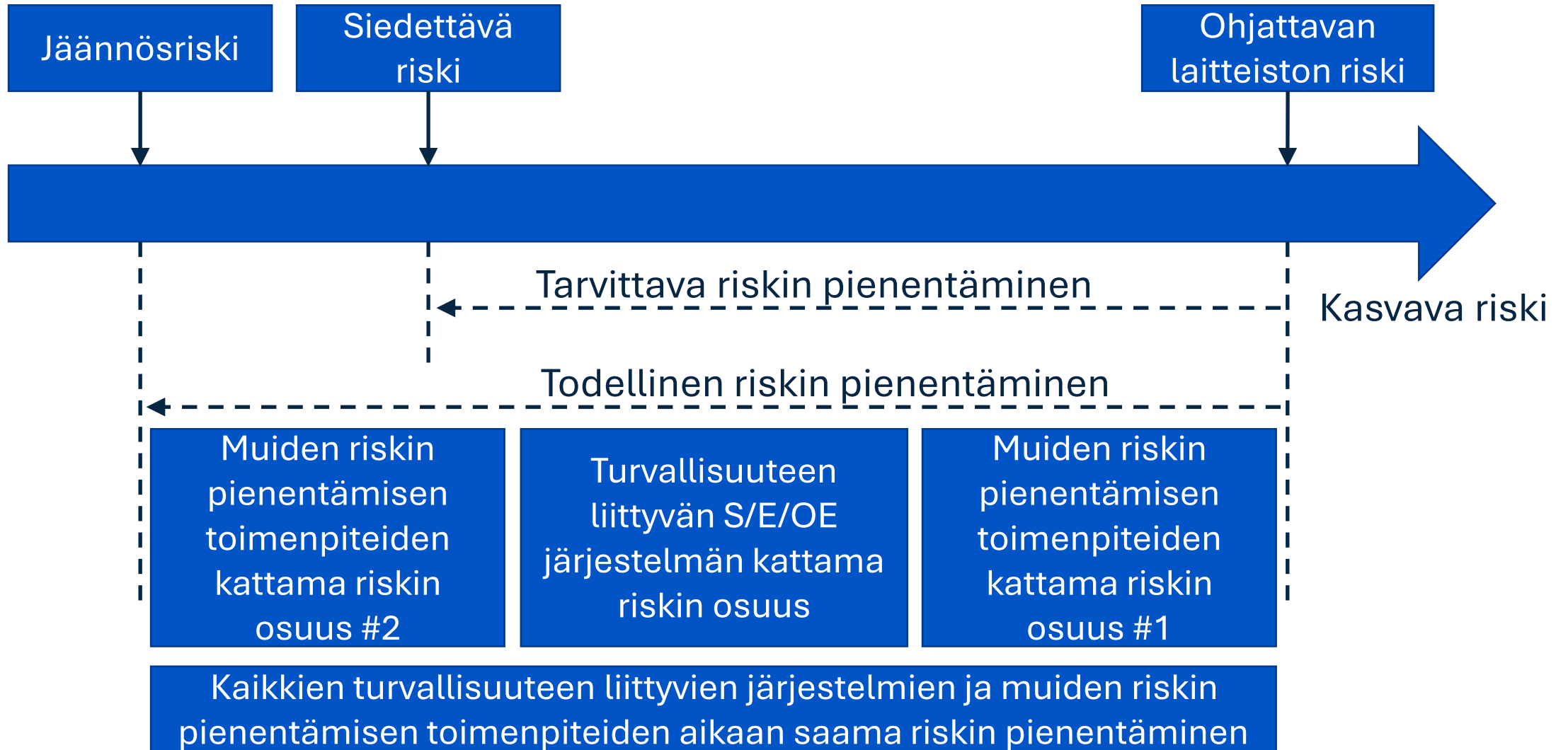
- (jatkoa edelliseltä kalvolta)
- Erityistä huomiota on kiinnitettävä seuraaviin seikkoihin:
 - a) kone tai vastaava tuote ei saa käynnistyä odottamattomasti;
 - b) koneen tai vastaavan tuotteen parametrit eivät saa muuttua hallitsemattomasti, jos tällainen muutos voisi aiheuttaa vaaratilanteita;
 - c) koneen tai vastaavan tuotteen tai käyttäjien tekemät muutokset asetuksiin tai sääntöihin, mukaan lukien koneen tai vastaavan tuotteen oppimisvaiheen aikana, on estettävä, jos tällaiset muutokset voisivat aiheuttaa vaaratilanteita;
 - d) koneen tai vastaavan tuotteen pysähtymistä ei saa estää, jos pysäytyskäsky on jo annettu;

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveyst- ja turvallisuusvaatimukset Ohjausjärjestelmän vaatimusten lisäykset alleviivattuna

1.2.1 Ohjausjärjestelmien turvallisuus ja toimintavarmuus

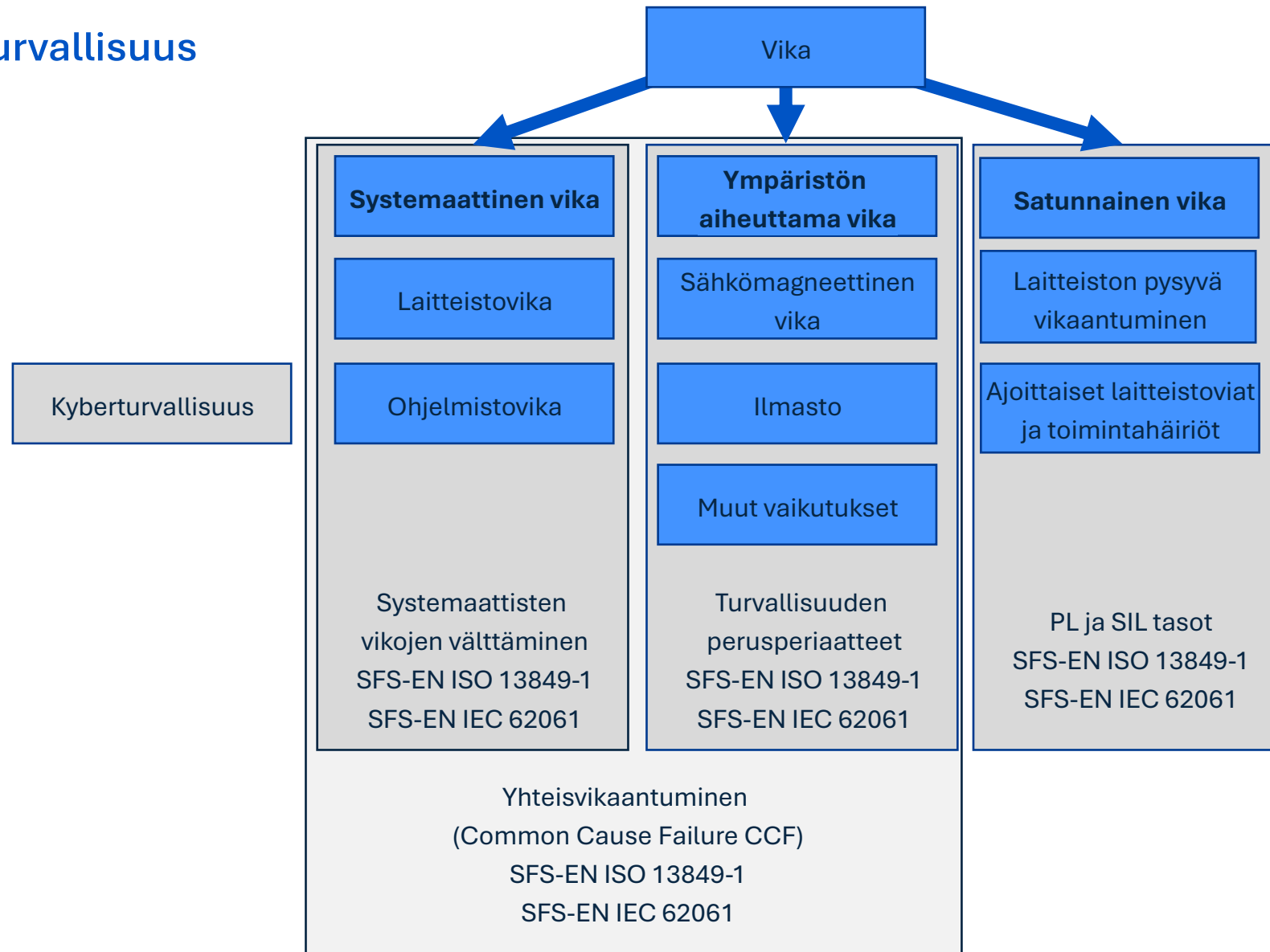
- (jatkoa edelliseltä kalvolta)
- e) mikään koneen tai vastaavan tuotteen liikkuva osa tai koneen tai vastaavan tuotteen kiinni pitämä kappale ei saa pudota tai sinkoutua;
- f) minkään liikkuvan osan automaattinen tai käsikäyttöinen pysäyttäminen ei saa estyä;
- g) turvalaitteiden on pysyttävä täysin toimintakykyisinä tai annettava pysäytyskäsky;
- h) turvallisuuteen liittyviä ohjausjärjestelmän osia on käytettävä yhtenäisellä tavalla koko koneyhdistelmään tai vastaaviin tuotteisiin tai osittain valmiisiin koneisiin, tai niiden yhdistelmään.
- Langattoman ohjauksen tiedonsiirron tai liitännän vikaantuminen tai viallinen yhteys ei saa aiheuttaa vaaratilannetta.

Riskin pienentäminen ja toiminnallinen turvallisuus (SFS-EN IEC 61508-5)



Huom. S/E/OE = sähköinen/elektroninen/ohjelmoitava elektroninen

Vikaturvallisuus



Toiminnallisen turvallisuuden saavuttaminen – systemaattinen kyvykkyys

Systemaattinen kyvykkyys (systematic capability, SC)

- Valittujen laitteiden tulee soveltua aiottuun käyttöön määritellyissä ympäristöolosuhteissa ja aiotun eheystason/suoritustason turvatoimintojen toteuttamiseen
- Laadun ja turvallisuuden hallinnan tulee täyttää aiotun eheystason tai suoritustason vaatimukset

SFS-EN IEC 62061:2021

- Kohta 6.5 Vaatimukset turvallisuuteen liittyvän ohjausjärjestelmän (SCS) systemaattiselle turvallisuuden eheydelle ja vaatimus toiminnallisen turvallisuuden suunnitelmasta
- Liitteessä I esimerkki turvallisuussuunnitelmasta

SFS-EN ISO 13849-1:2023

- Kohta 10.6.2 Toimenpiteet systemaattisen vikaantumisen estämiseksi sekä liitteen G lisätoimenpiteet
- Liitteessä G suositellaan toiminnallisen turvallisuuden hallintaa

Toiminnallisen turvallisuuden saavuttaminen – rakenteelliset rajoitukset

Rakenteelliset rajoitukset (architectural constraints, AC)

- Rakenteen tulee täyttää aiotun eheystason tai suoritustason rajoitukset ja vaatimukset
- Laitteiston vikasietoisuus (HFT) on oltava suoritustason tai eheystason asettamissa rajoissa

SFS-EN IEC 62061:2021

- Esittää tietylle eheystasolle vaaditun vikasietoisuuden (HFT) perustuen turvallisten vikaantumisten osuuteen (SFF)
- Periaate on kattostandardin IEC 61508 mukainen

SFS-EN ISO 13849-1:2023

- Esittää vaaditun vikasietoisuuden perustuen luokkien mukaisten nimettyjen rakenteiden soveltamiseen
- Asettaa suurimman saavutettavissa olevan suoritustason luokille

Toiminnallisen turvallisuuden saavuttaminen – tavoitteellinen vikaantumismitta

Tavoitteellinen vikaantumismitta (average frequency of a dangerous failure per hour, PFH)

- Rakenteen tulee täyttää aiotun eheystason tai suoritustason tavoitteellinen vikaantumismitta
- Vaarallisten vikaantumisten todennäköisyys satunnaisten laitteiston vikaantumisten osalta osoitetaan luotettavuustekniikan analyttisin menetelmin

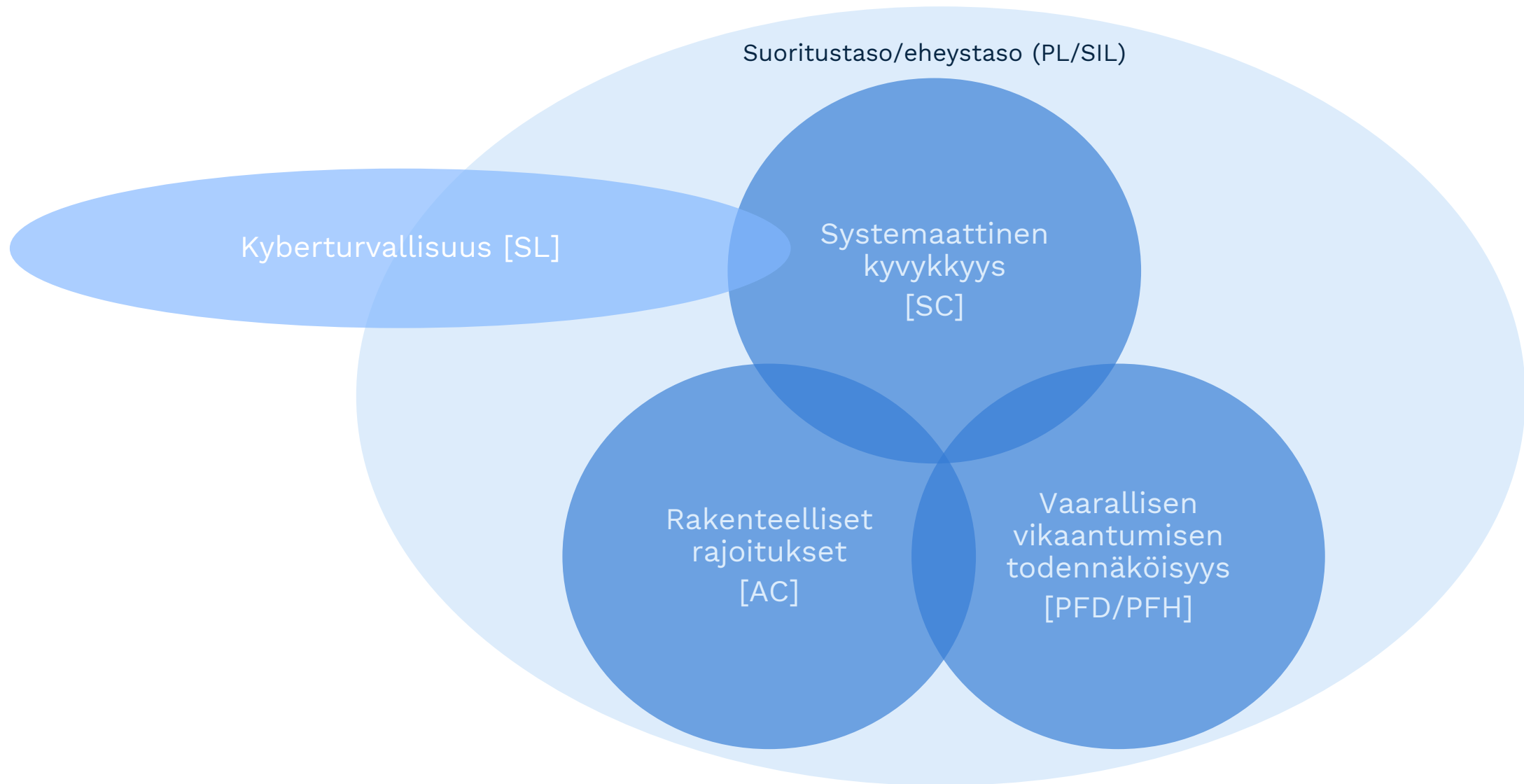
SIL	PFH-arvojen raja (1/h)
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

Kuva: SFS-EN IEC 62061:2021

PL	Vaarallisen vikaantumisen keskimääräinen taajuus tunnissa (PFH) 1/h
a	$10^{-5} \leq \text{PFH} < 10^{-4}$
b	$3 \times 10^{-6} \leq \text{PFH} < 10^{-5}$
c	$10^{-6} \leq \text{PFH} < 3 \times 10^{-6}$
d	$10^{-7} \leq \text{PFH} < 10^{-6}$
e	$\text{PFH} < 10^{-7}$

Kuva: SFS-EN ISO 13849-1:2023

Toiminnallisen turvallisuuden saavuttaminen



Mitä on kyberturvallisuus?

- Pää tavoitteena kyberturvallisuudessa on estää pahantahtoisen toiminnan aiheuttamat vahingot.
- Kyberturvallisuus on suhteellisen uusi ja sisällöltään vielä vakiintumaton termi. Määritelmiä on lukuisia erilaisia, esimerkiksi: *”Käytännössä kyberturvallisuudella viitataan organisaatioiden ja yhteiskunnan digitalisoitumisen aiheuttamiin uudenlaisiin turvallisuushaasteisiin.”*

Kyberturvallisuuslaki 124/2025, 2 §, Määritelmät

- *Tässä laissa tarkoitetaan:*
- ...
- *7) kyberturvallisuudella toimia, joita tarvitaan viestintäverkkojen ja tietojärjestelmien, niiden käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta*

EU:n kyberturvallisuusasetus (EU) 2019/881, 2 artikla, Määritelmät

- *Tässä asetuksessa tarkoitetaan:*
- *1) ’kyberturvallisuudella’ toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta;*

Perusteita

Kyberturvallisuus: koneiden turvallisuutta koskeva lainsäädäntö edellyttää koneiden ohjausjärjestelmien valmistajilta vähintäänkin oikeasuhteisia toimenpiteitä tuotteen turvallisuuden suojeluun

- EU:n kyberturvallisuusasetuksessa (CSA) (EU) 2019/881 on määritelty EU:n laajuisten kyberturvallisuuden sertifiointijärjestelmien kehittäminen ja käyttöönotto.
- EU:n kyberturvallisuusedirektiivin (NIS2) (EU) 2022/2555 ja Suomen kyberturvallisuuslain 124/2025 tavoitteena on kyberturvallisuuden yhteisen korkean tason varmistaminen kaikkialla Euroopan unionissa.
- EU:n yleisen tuoteturvallisuusasetuksen (GPSR) (EU) 2023/988 tavoitteena on varmistaa, että kaikki EU:n markkinoilla olevat kuluttajatuotteet ovat turvallisia. Asetus huomioi kyberturvallisuusominaisuudet, jotka ovat tarpeen tuotteen suojaamiseksi ulkoisilta vaikutuksilta.
- EU:n kyberkestävyyssäädöksen (CRA) (EU) 2024/2847 tavoitteena on parantaa EU:n markkinoille saatettujen tuotteiden tietoturvaa niin, että tuotteissa on vähemmän haavoittuvuuksia.
 - Asettaa olennaiset kyberturvallisuusvaatimukset.
- EU:n koneasetus (EU) 1230/2023, 20 artikla, kohta 9.: *”Koneita ja vastaavia tuotteita, jotka on sertifioitu tai joista on annettu vaatimustenmukaisuusilmoitus sellaisen asetuksen (EU) 2019/881 mukaisesti hyväksytyn kyberturvallisuuden sertifiointijärjestelmän nojalla, jonka viitetiedot on julkaistu Euroopan unionin virallisessa lehdessä, on pidettävä liitteessä III olevissa 1.1.9 ja 1.2.1 kohdassa esitettyjen olennaisten terveys- ja turvallisuusvaatimusten mukaisina tietojen turmeltumiselta suojautumisen sekä ohjausjärjestelmien turvallisuuden ja toimintavarmuuden osalta siltä osin kuin kyberturvallisuus-sertifikaatti tai vaatimustenmukaisuus ilmoitus tai niiden osat kattavat kyseiset vaatimukset.”*

EU:n koneasetus (EU) 2023/1230 – Olennaiset terveys- ja turvallisuusvaatimukset

Kyberturvallisuuden vaatimuksen lisäys ilman rajausta ohjausjärjestelmään

1.1.9 Suojaus tietojen turmeltumista vastaan

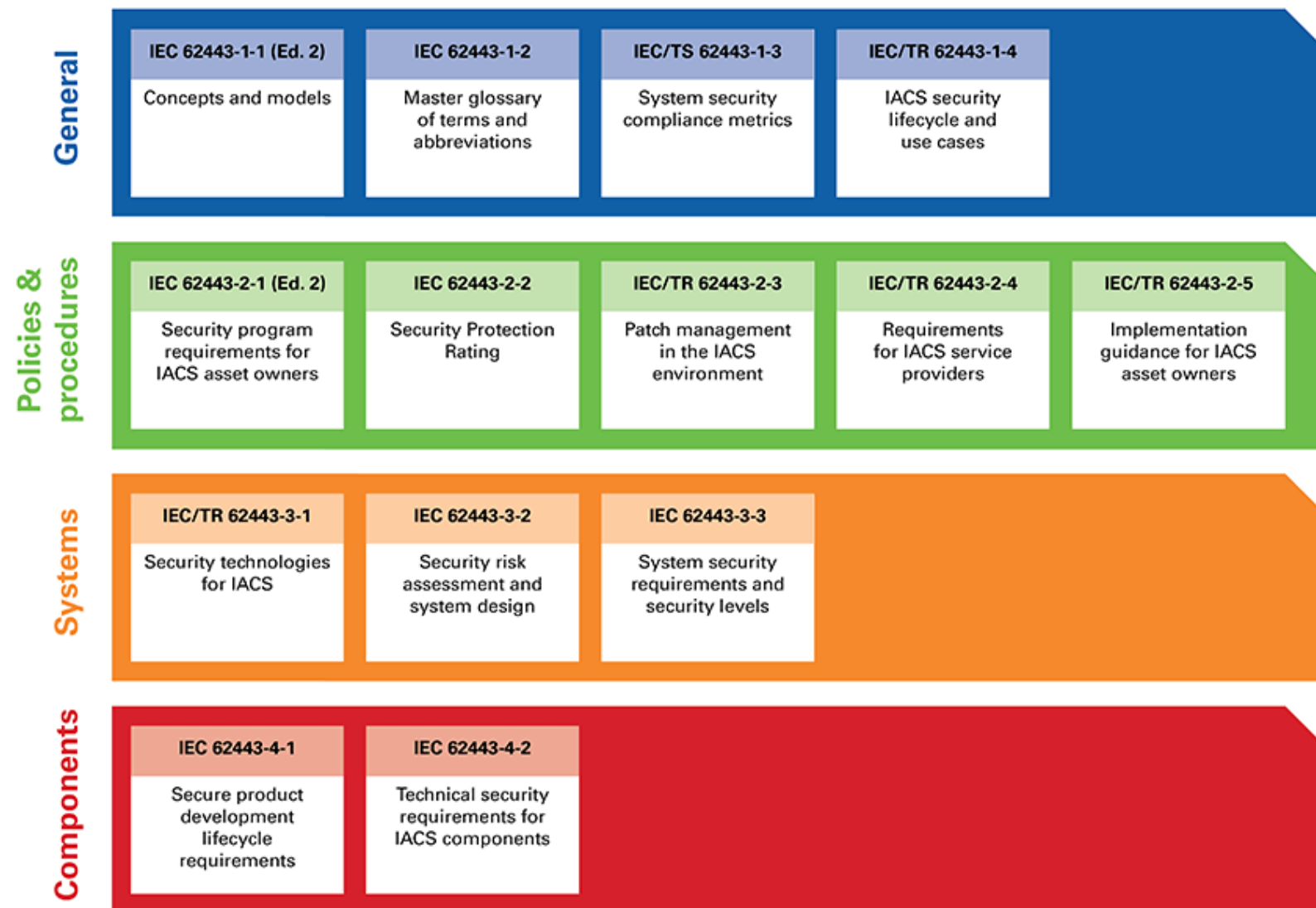
- Kone tai vastaava tuote on suunniteltava ja rakennettava siten, että sen liittäminen toiseen laitteeseen, joko liitetyn laitteen jonkin oman ominaisuuden kautta tai jonkin koneen tai vastaavan tuotteen kanssa kommunikoivan etälaitteen välityksellä, ei aiheuta vaaratilannetta.
- Ohjelmistoliitintä tai ohjelmiston käyttöä varten tarvittava laitteistokomponentti, joka välittää signaalin tai dataa ja joka on kriittinen sen kannalta, että kone tai vastaava tuote on asiaankuuluvien olennaisten terveys- ja turvallisuusvaatimusten mukainen, on suunniteltava siten, että se on riittävästi suojattu tarkoitukselliselta tai vahingossa tapahtuvalta tietojen turmelemiselta. Koneen tai vastaavan tuotteen on kerättävä näyttöä perustellusta tai perusteettomasta sellaiseen laitteistokomponenttiin puuttumisesta, joka on kriittinen koneen tai vastaavan tuotteen vaatimustenmukaisuuden kannalta.
- Ohjelmistoissa ja datassa, jotka ovat kriittisiä sen kannalta, että kone tai vastaava tuote on asiaankuuluvien olennaisten terveys- ja turvallisuusvaatimusten mukainen, on oltava tästä maininta, ja ne on suojattava riittävästi tarkoitukselliselta tai vahingossa tapahtuvalta tietojen turmelemiselta.
- Koneen tai vastaavan tuotteen on yksilöitävä siihen asennettu ohjelmisto, joka on välttämätön sen turvallisen toiminnan kannalta, ja sen on kyettävä milloin tahansa antamaan tämä tieto helposti saatavilla olevassa muodossa.
- Koneen tai vastaavan tuotteen on kerättävä näyttöä perustellusta tai perusteettomasta puuttumisesta koneeseen tai vastaavaan tuotteeseen tai koneeseen tai vastaavaan tuotteeseen asennetun ohjelmiston tai sen kokoonpanon perustellusta tai perusteettomasta muuttamisesta.

Käännös!

Standardit työkaluina EU:n kyberturvallisuusvaateiden täyttämiseksi

- Kyberturvallisuusvaatimuksia on lukuisissa eri standardeissa ja EU:n alueella yhdenmukaistettua standardia ei ole.
- Standardi ISO/IEC 27001 on vakiintunut tietoturvallisuuden hallintajärjestelmien sertifiointissa.
- CEN ISO/TR 22100-4 antaa ohjeita koneiden valmistajille kyberturvallisuuteen liittyviin näkökohtiin.
 - Esittää uhkan vaikutusmahdollisuuden suunnittelijan toteuttamiin suojaustoimenpiteisiin.
 - Esittää olennaiset toimenpiteet tietoturvallisuuden käsittelemiseksi koneen koko elinkaaren ajan.
- Ohjausjärjestelmästandardi SFS-EN IEC 62061 viittaa tietoturvallisuusstandardiin ISO/IEC 27001, IEC 62443 standardisarjaan sekä erilaisiin teknisiin raportteihin.
- IEC 62443 standardisarja on laajasti käytetty ja hyväksytty markkinoilla.
 - Standardisarjan useat osat ovat saavuttaneet EN-standardin aseman.
 - Standardisarjan useat osat on käännetty suomen kielelle.
 - Standardisarjan osat -3-3, -4-1, sekä -4-2 ovat CRA asetuksen kannalta asiaankuuluvia.
- Tekeillä on kriittisten/tärkeiden koneiden kyberturvallisuusstandardi, jonka luonnosversio on prEN 50742. Tavoitteena on saavuttaa EU:n koneasetuksen alainen yhdenmukaistettu standardi.
- Kyberturvallisuuden standardointi on kypsymätöntä verraten toiminnallisen turvallisuuden standardointiin ja järkeistäminen on tarpeen resurssien kohdentamisessa.

IEC 62443 standardisarja elinkaaren tietoturvallisuuden hallintaan



Kuvat: kiwa.com, enisa

Kyberturvallisuusriskien arviointi

Uhkien ja riskien tunnistaminen

- Suojattavien kohteiden tunnistaminen ja yksilöinti
- Uhkien ja haavoittuvuuksien tunnistaminen ja yksilöinti sekä riskien luokittelu
- Alihankintaketjujen tunnistaminen ja yksilöinti
- Arkkitehtuurin kuvaus ja liityntöjen yksilöinti sekä järjestelmän jakaminen vyöhykkeisiin ja tietoväyliin

Riskien merkityksien arviointi ja vastatoimenpiteiden tehokkuus

- Elinkaaren hallintamallin kuvaus sekä roolien ja vastuiden tunnistaminen ja yksilöinti
- Tietoturvasojen määrittely
- Komponenttivalmistajien, järjestelmäintegraattorin, ylläpitopalveluiden tarjoajan ja suojattavien kohteiden omistajan tehtävät
- Fyysisen tietoturvallisuuden keinot (kulunvalvonta, pääsyn hallinta, eristäminen)
- Teknisen tietoturvallisuuden keinot (tekniset suunnitteluratkaisut, testaus)
- Hallinnollisen tietoturvallisuuden keinot (prosessit, menettelytavat)

IEC 62443 standardisarjan perustavanlaatuiset vaatimukset (FR) ja tietoturvan tasot (SL)

IEC 62443-1-1 asettaa perustavanlaatuiset tietoturvavaatimukset (FR): pääsyn valvonta (AC), käytön valvonta (UC), tiedon eheys (DI), tiedon luottamuksellisuus (DC), rajoitettu tiedon virtaus (RDF), nopea reagointi tapahtumaan (TRE), resurssien saatavuus (RA).

IEC 62443-3-2 antaa menettelyn tietoturvasojen tavoitteiden (SL-T) määrittämiseen.

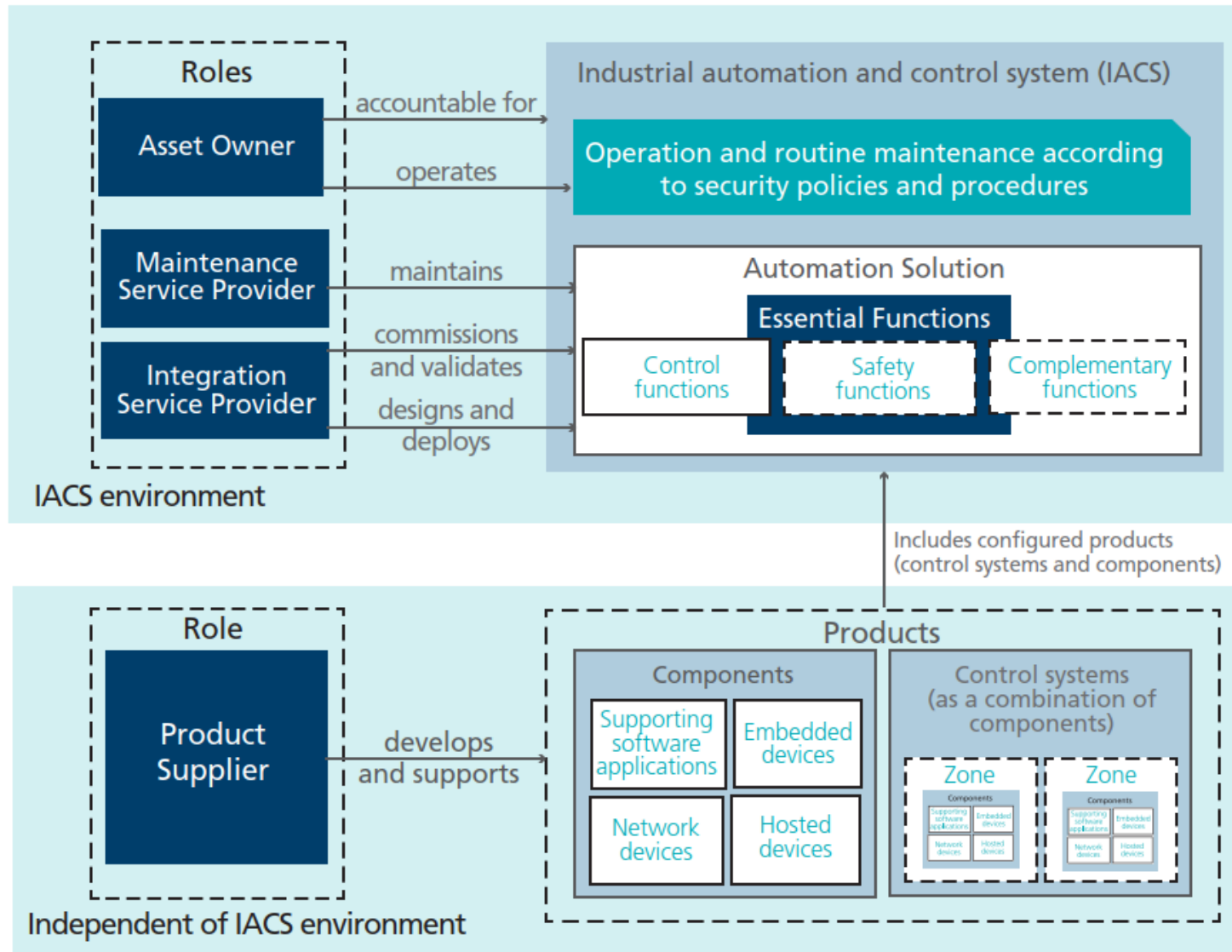
IEC 62443-3-3 asettaa yksityiskohtaiset järjestelmävaatimukset (SR) sekä niiden laajennukset (RE) tietoturvasojen kyvykkyydelle (SL-C) tai saavutukselle (SL-A).

Vyöhykkeelle tai tietoväylälle asetettavat tietoturvasoot:

- SL 1 : Estä tietojen luvaton paljastaminen salakuuntelun tai satunnaisen altistumisen avulla.
- SL 2 : Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle yksinkertaisilla keinoilla, joilla on vähän resursseja, hieman taitoja ja alhainen motivaatio.
- SL 3 : Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle kehittyneillä keinoilla, joilla on kohtuulliset resurssit, IACS -erityistaitoja ja kohtalainen motivaatio.
- SL 4 : Estä tietojen luvaton paljastaminen sitä aktiivisesti etsivälle yhteisölle kehittyneillä keinoilla, joilla on laajat resurssit, IACS -erityistaitoja ja korkea motivaatio.

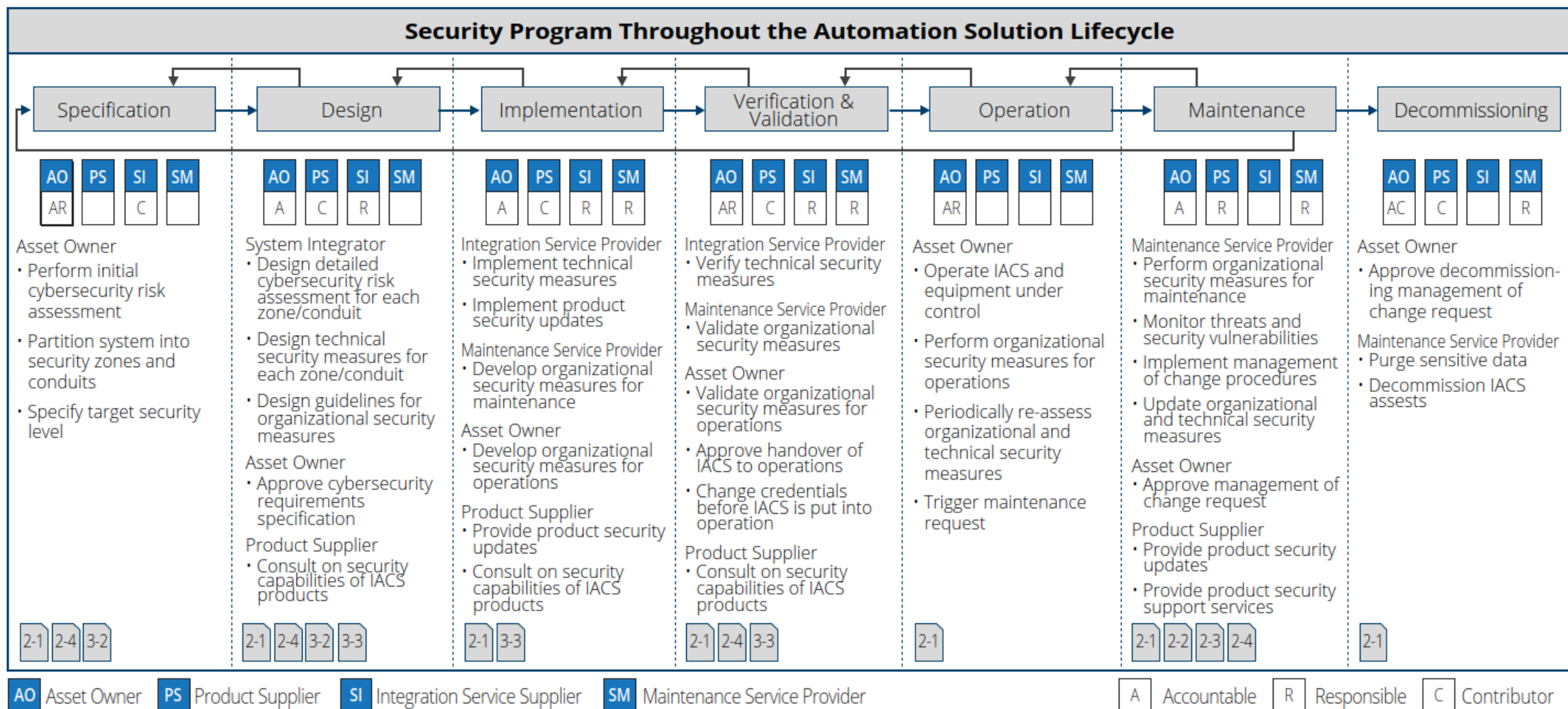
Saavutettu tietoturvaso (SL-A) on ajan funktio, ja se alenee ajan kuluessa.

IEC 62443 standardisarjan perustavanlaatuiset roolit ja vastuut



Kuva: www.isa.org/ISAGCA

IEC 62443 standardisarjan kyberturvallisuusohjelma automaattioratkaisun elinkaaren läpi



Turvallisuuteen liittyvän ohjausjärjestelmän toiminnallisen turvallisuuden ja kyberturvallisuuden integraatio

- Toiminnallisen turvallisuuden hallinnan elinkaarimalli antaa hyvän pohjan kyberturvallisuuden hallinnalle.
 - SFS-EN IEC 62061 perustuu kattostandardin IEC 61508 elinkaarimalliin.
 - SFS-EN ISO 13849 tunnistaa elinkaarimallin ohjelmiston osalta.
 - IEC TR 63069 / IEC TS 63069 kehitystyö on esimerkki yhteisestä kehyksestä ja koordinaatiosta.
- Hallintajärjestelmien kustannustehokas toteutus edellyttää toiminnallisen turvallisuuden hallinnan ja kyberturvallisuuden hallinnan integrointia. Tehokkaan integraation mahdollistamiseksi haavoittuvuus kyberhyökkäyksille on tarpeen huomioida jokaisessa toiminnallisen turvallisuuden elinkaaren vaiheessa.
- Ohjattavan laitteiston riskien edellyttämien suoritustasojen/eheystasojen vaateet on kyettävä erottelmaan kyberturvallisuusriskien edellyttämien tietoturvasojen vaateista. “Turvallisuus ensin”.
- Useat turvallisuuteen liittyvän ohjausjärjestelmän systemaattisen kyvykkyyden saavuttamiseksi tarvittavat toimenpiteet ovat samankaltaisia kuin kyberhyökkäyksiltä suojautumiseksi tarvittavat toimenpiteet. Ohjelmistojen laadunhallinta tukee sekä toiminnallista turvallisuutta, että kyberturvallisuutta, esimerkiksi
 - SFS-EN IEC 62061 edellyttää kokoonpanon hallintaa (ja SFS-EN ISO 13849 sulautetuille ohjelmistoille).
 - SFS-EN IEC 62061 ja SFS-EN ISO 13849 edellyttävät valtuuttamattoman pääsyn/muuttamisen estoa.

Kiitos mielenkiinnosta!

Janne Peltonen
Asiantuntija, Automaatioturvallisuus
T +358 50 302 5280
E janne.peltonen@kiwa.com