Suomen Automaatioseura ry
Finnish Society of Automation

Suomen Automaatioseura ry Turvallisuusjaos Automation Safety Forum (ASAF)

SIL-normitalkoot

Janne Peltonen, Fennovoima, 11.5.2020

Huomautus:
Esitys on laadittu Automaatioseuran turvallisuusjaoston yhteistyötavoitteisen keskustelun pohjaksi.
Esitys ei edusta esittäjän työnantajan näkemyksiä tai kannan ottoja minkään toimialan standardoinnin osalta.

ASAF missio

Suomen Automaatioseura ry
Finnish Society of Automation

Keskeinen kysymys automaation turvallisuudessa on turvatoimintojen toteuttaminen ohjelmoitavien elektronisten järjestelmien avulla sekä langattoman ja etäohjauksen turvallisuus.

Turvallisuusjaoston tarkoituksena on kehittää yhteistoimintaa ja koota yhteen automaation turvallisuusasiantuntemusta eri tahoilta.

Jaoston lähtökohtana on automaatiojärjestelmien henkilöturvallisuus. Keskeisiä teemoja ovat:

- riskin arviointi
- turvallisuuden eheyden tasot
- turvallisuuden hallintajärjestelmät
- käyttöliittymät
- turvajärjestelmät ja -laitteet
- turvallisuuteen liittyvät säädökset ja standardit
- automaation laatu
- automaation tietoturva
- kelpoistus ja sertifiointi
- koulutus

Lainaus SFS-EN 61508 esipuheesta

*Useimmissa tapauksissa turvallisuus saavutetaan usealla järjestelmällä, jotka perustuvat moneen teknologiaan (esimerkiksi mekaaniseen, hydrauliseen, pneumaattiseen, sähköiseen, elektroniseen, ohjelmoitavaan elektroniseen). Niinpä turvallisuusstrategian täytyy huomioida ei vain yksittäisen järjestelmän kaikki elementit (esimerkiksi tuntoelimet, ohjauslaitteet ja toimilaitteet), vaan myös kaikki turvallisuuteen liittyvät järjestelmät, jotka muodostavat turvallisuuteen liittyvien järjestelmien koko yhdistelmän. Näin ollen, vaikka tämä kansainvälinen standardi ottaa kantaa S/E/OE turvallisuuteen liittyviin järjestelmiin, se **saattaa** tarjota myös puitteet, joissa muihin teknologioihin pohjautuvia turvallisuuteen liittyviä järjestelmiä voidaan tarkastella.*

Pohdinta

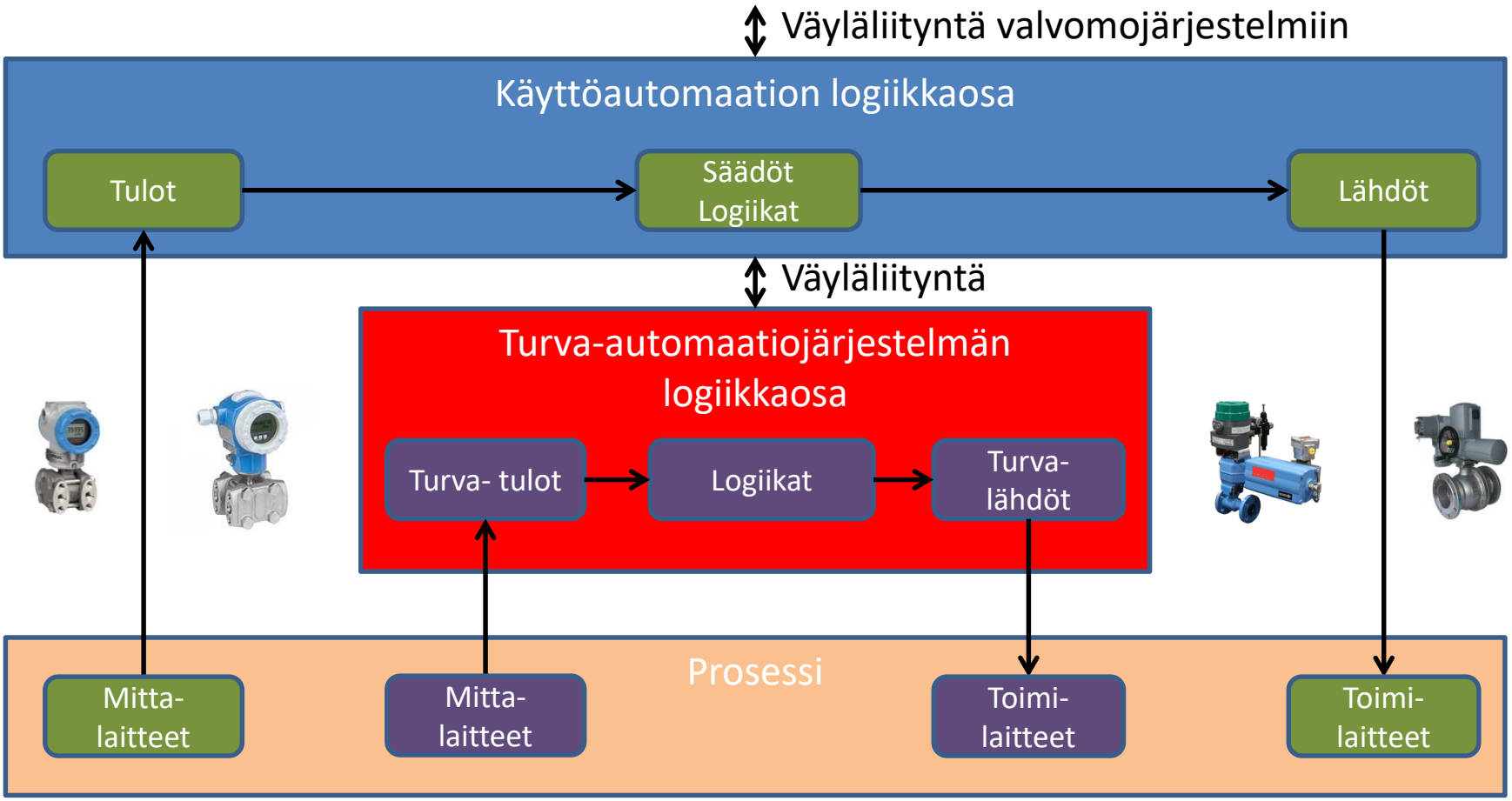
- SFS-EN 61508 (IEC 61508) kattostandardi ja sovellusalakohtaiset standardit määrittelevät yleisesti tunnustetun menettelytavan toiminnallisen turvallisuuden hallintaan, riskien pienentämiseen ja teknisten ratkaisujen arviointiin

- SIL-standardien soveltamisen mielekkyys ja kustannustehokkuus on pohdittavissa
  - Onko turvallisuustaso parantunut 20 vuodessa?
  - Tuottaako elinkaarimallin soveltaminen turvallisuustason parantumista suhteessa käytettyihin resursseihin?

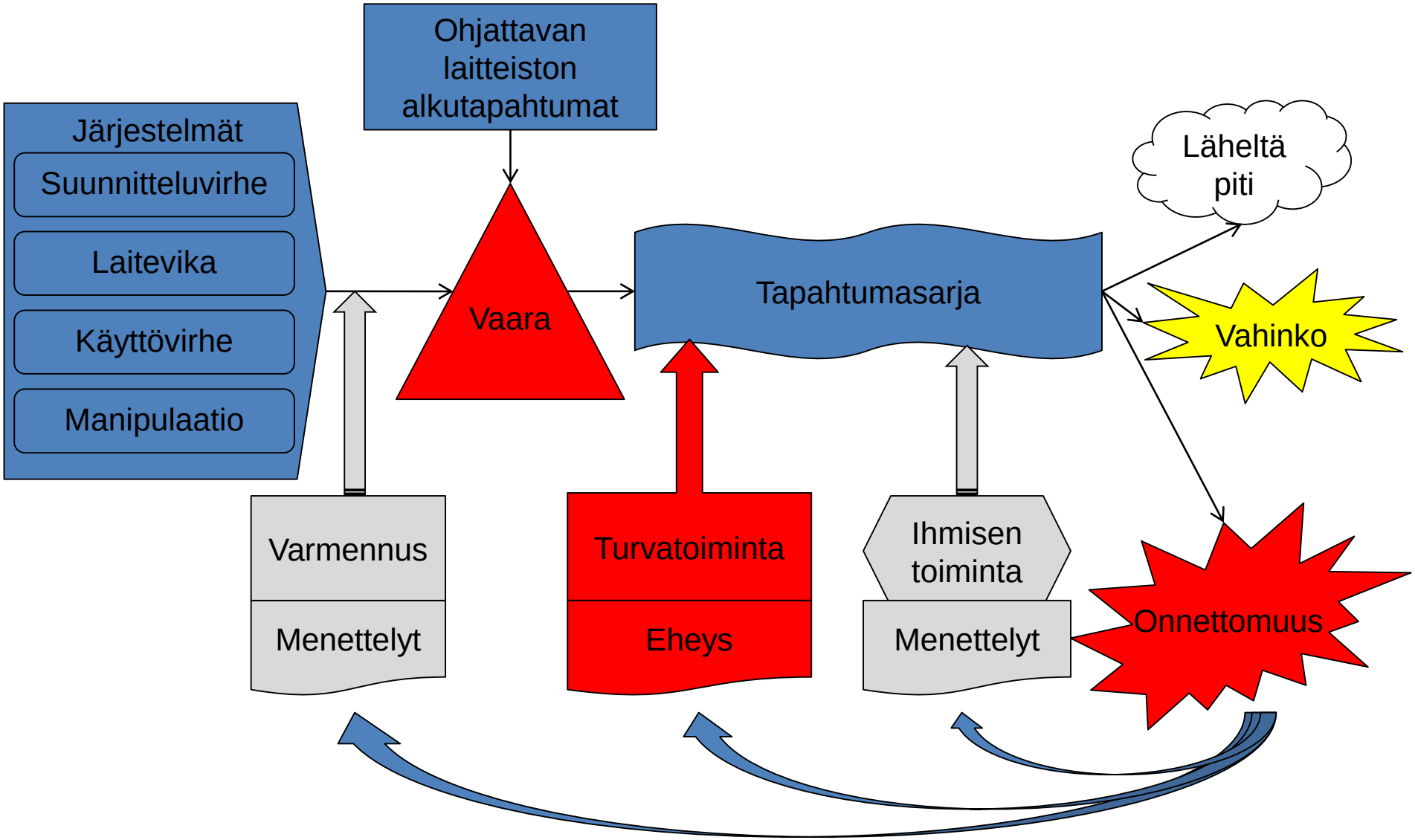
Toiminnallinen turvallisuus riskienhallinnassa

- Toiminnallisen turvallisuuden standardeissa on systemaattisesti omaksuttu riskilähtöinen lähestymistapa turva-automaation ratkaisujen toteutukseen
- Turvallisuusbudjetti on aina rajallinen
- Varautumiskeinojen toteutuksen kustannustaso tulee vastata toiminnassa koetun riskin suuruutta – myös tavanomainen käytön automatisointi on varautumista
- Toiminnalliset tekniset automaatiojärjestelmät varautumiskeinona pienentävät riskejä ja voivat luoda myös uusia **teknologialähtöisiä riskejä**
  - Jos sovellus on yksinkertainen, käytä yksinkertaista tekniikkaa
  - Ohjelmoitavan tekniikan käyttäminen luo sekä yhteisvikaantumisen mahdollisuuksia että tietoturvallisuusuhkia

Automaatiojärjestelmät

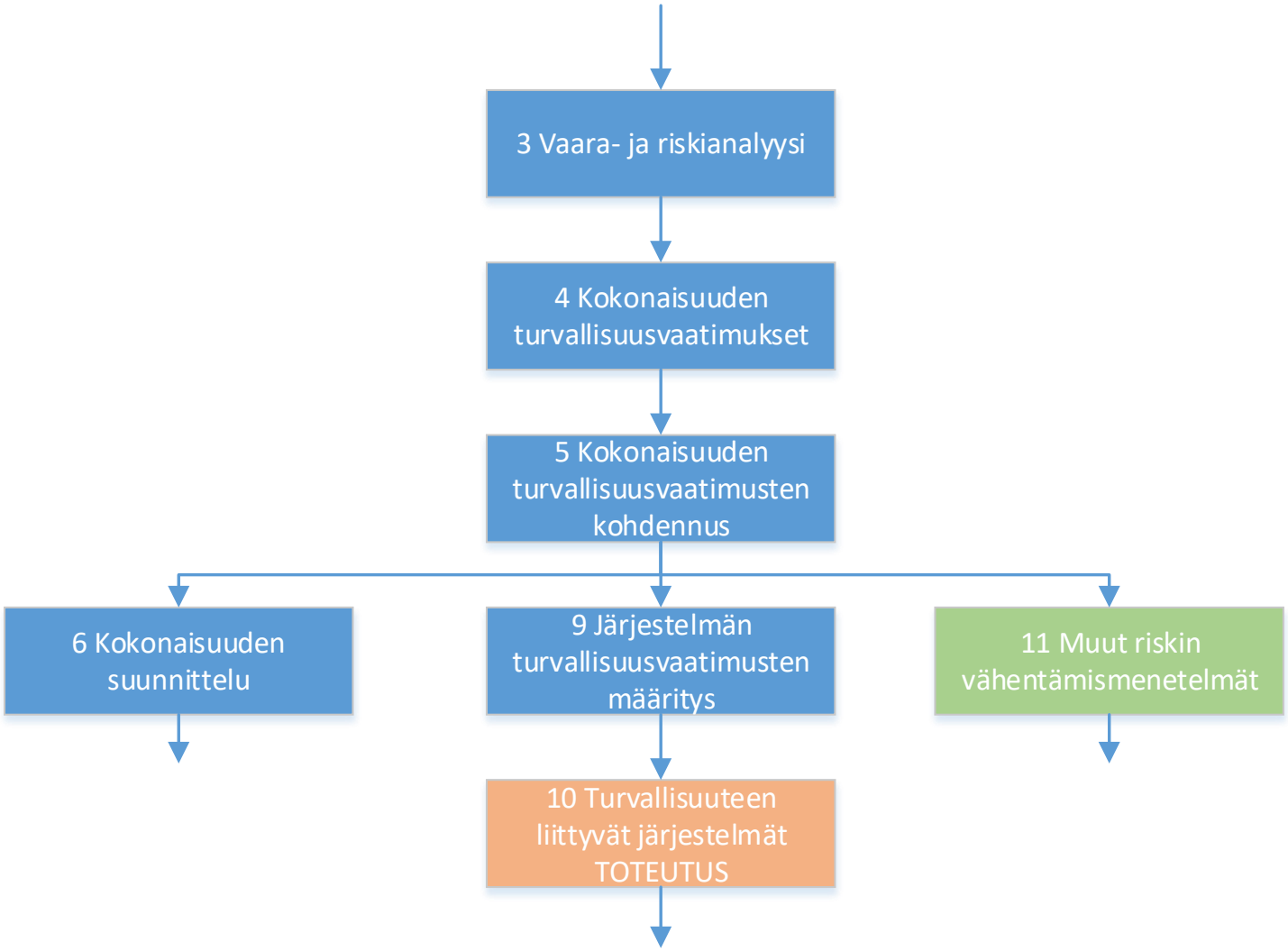


Toiminnallinen turvallisuus – takaisinkytkentä normeilla



Normit: säädökset, standardit, käytännesäännöt

SFS-EN 61508
Elinkaaren elintärkeät vaiheet

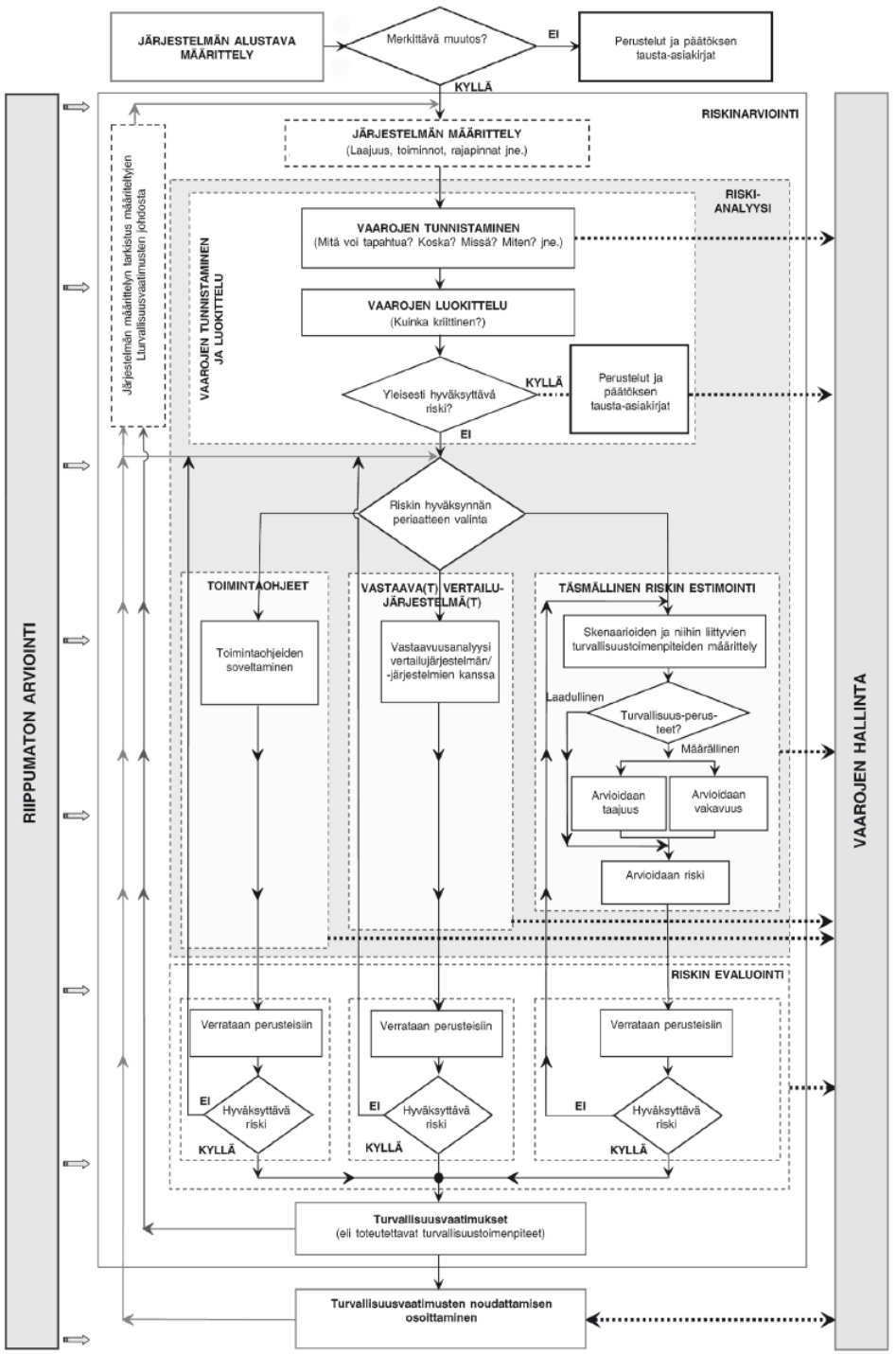


Huom. Kokonaisuuden suunnittelun soveltamisala on ohjattava laitteisto, ohjausjärjestelmät ja turvallisuuteen liittyvät järjestelmät

Vertailun vuoksi: Komission asetus (EU) N:o 402/2013

Riskin hyväksynnän periaatteen valinta:

- Toimintaohjeet
- Vertailujärjestelmät
- Täsmällinen estimointi



SFS-EN 61508
Peruskäsitteiden peruskysymyksiä

IEC 61508 esittää riskipohjaisen lähestymistavan sekä teknologisista ratkaisuista riippumattomat suorituskykypohjaiset vaatimukset.

- Kuka laatii laitoksen turvallisuussuunnittelun ohjeen/oppaan/standardin?
  - S/E/OE järjestelmät ovat vaihtoehtoja muiden joukossa (pataraudan paksuus vs. SIL-toiminnot)
- Kuka määrittelee konseptin ja kokonaisuuden soveltamisalan, jonka riskiä pyritään pienentämään?
- Kuka määrittelee siedettävän riskin?
- Mihin suorituskyvyn (SIL) riittävyyttä verrataan?
- Kuka hyväksyy saavutetun (t.s. riittävästi pienennetyn) riskitason?

IEC 61508 määrittelee turvallisuuden eheyden tasot (SIL), joita soveltamalla sopiva turvallisuuden eheyden taso turvatoiminnoille voidaan valita riskin pienentämisen tarpeen mukaisesti.

- Onko tavanomaisten toimintojen (”SIL 0”) riskin pienentäminen huomioitavissa?
- Onko eheysvaatimuksien (SIL) allokoinnissa huomioitu eri suojauskerrokset?
- Onko eheysvaatimuksien (SIL) allokoinnissa huomioitu rinnakkaiset toiminnot?
- Onko eheysvaatimuksien (SIL) allokoinnissa huomioitu järjestelmäkokonaisuus?
- Onko eheysvaatimukset (SIL) asetettu koko ketjulle ml. mitta- ja toimilaitteet?

Havaintoja SIL-ongelmista

- Turvatoimintojen todellista SIL-suorituskyvyn tarvetta ei tiedetä
  - Turvatoimintojen tunnistaminen jää vajaaksi, jolloin vaarojen ja turvatoimintojen yhteyttä ei tunnisteta johdonmukaisesti
  - Siedettävää riskiä ei kyetä määrittelemään
  - Vaatimusviidakko kasvaa ja kehittyy vuosikymmenestä toiseen
  - Kokonaisuuden turvallisuutta ja päätöksentekoa ei tiedetä
  - Turvallisuusvaatimukset ja ratkaisut kopioidaan muualta

- Turvatoimintojen todellista SIL-suorituskykyä ei tiedetä
  - Toimialan laajuisesti ei kyetä mittaamaan SIL-suorituskykyä
  - Valmistajat laskevat oletuksin komponenttien SIL-suorituskyvyn
  - Sovelluskohtaiset ratkaisut voivat parantaa tai rikkoa suorituskykyä

Havaintoja SIL-ongelmista

- Turvatoimintojen kohdentaminen on yksinkertaistettua tai suoraviivaistettua
  - Copy-paste arkkitehtuuriset ratkaisut ilman analyyseja
  - Suorituskyvyn osoittaminen annetaan toimittajan ongelmaksi
  - Mallintamiselle riskinarvioinnin tueksi ei ole resursseja
  - Vaatimustasoa ei osata lieventää arkkitehtuurin avulla
  - Vaatimustasoa lievennetään liikaa virheellisillä menettelyillä

- Turvatoimintojen vaatimusmäärittelyjä ei kyseenalaisteta
  - Vaatimusten hallinta ja laadukas kirjaus on työlästä ja kallista
  - Vaatimukset ja tekniset ratkaisut sekoitetaan samaan soppaan
  - Sopimustekniset rajat estävät ongelmiin puuttumisen tai korjauksen
  - Mallintamiselle tai simuloinnille ei ole resursseja

Havaintoja SIL-ongelmista

- Yleisesti standardoinnin soveltaminen kohdentuu liiaksi toimittajiin/toimituksiin
  - Loppukäyttäjä, aiottu käyttötarkoitus ja suojausten kokonaisuus ovat olennaisia kokonaisuuden turvallisuuden kannalta
  - Dokumentoidun näytön tulisi olla samalla tasolla koko elinkaaren yli
  - Järjestelmän käytön, ylläpidon ja muutosten vastuut koko elinkaaren yli tulee olla järjestettävissä
- SIL-standardit pyrkivät yhdistämään organisaatioiden toiminnan ja tekniset suunnitteluratkaisut dokumentoidusti, mikä saattaa rajoittaa olennaisesti organisaatioiden vapaata toimintaa ja kehitystä
  - Vaivalla dokumentoituja prosesseja ei haluta enää muuttaa
  - Seurauksena tai sivutuotteena voi olla älyvapaata toimintaa
- SIL-standardit antavat kokonaiskehyksen, mutta eivät huomioi ihan kaikkea
  - Prosessi- ja sähkösuunnittelun elinkaarimalleja ei ole standardoitu rinnalle
  - Inhimilliset tekijät otetaan huomioon kokemuksen avulla
  - Tietoturvallisuus oletetaan sisään rakennetuksi
  - Konfiguraation hallinta käsitetään ohjelmoitavan tekniikan asiaksi

SIL-normitalkoiden tarve?

- SIL-standardien soveltaminen koetaan hankalaksi, jäykäksi, monimutkaiseksi, byrokraattiseksi ja kalliiksi
  - Standardien laatijat itsekin toivoisivat yksinkertaistusta?
  - Standardit kirjoitetaan ”kuvitteellisessa ideaalimaailmassa”?
  - Haaveissa paluu menneisyyteen ennalta normitettujen keittokirjojen äärelle?
  - Yrityskohtaisia riskimatriiseja tai suunnittelun kriteeristöjä ei osata tehdä?
  - Yrityskohtaisia standardin sovellutuksia toimintaohjeiden muodossa ei kannata tehdä?
  - Vaatimuksia kirjoitetaan vain organisaation ulkopuolelta käsin?
  - Elinkaarimallia ei ehditä käytännössä noudattaa?
  - Riittävä pätevyys poistaa tarpeen dokumentoida vaiheittaista toimintatapaa?
  - Standardien määrittelemien roolien ja tehtävien yksityiskohtainen ”atomisointi” raskauttaa koko elinkaariprosessia tarpeettomasti?
  - Elinkaarimallin tehtäviä ei pystytä sopeuttamaan turvallisuustasoon?

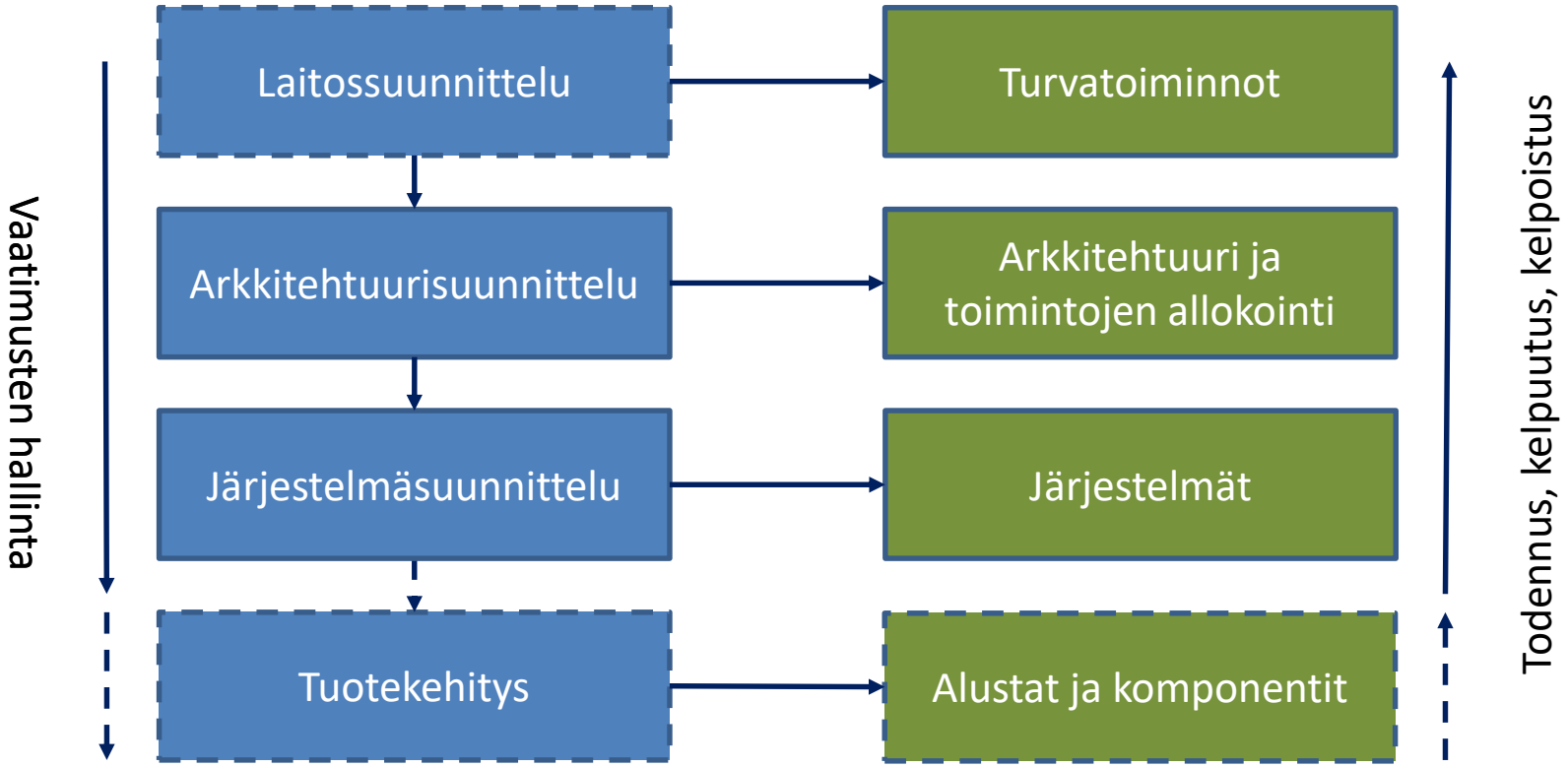
Aikuisten oikeasti siis…

- Itse asiassa IEC 61508-perhe ja toiminnallisen turvallisuuden SIL-standardit ovat harvinaisen hyvin tehtyjä, suorituskykypohjaisia, kattaviksi todistettuja sekä hyvin ylläpidettyjä standardisarjoja!

- Elinkaarimallin soveltaminen tyypillisesti tuottaa perusteltuja päätöksiä oikeassa kontekstissa
  - Vaiheittaiset vaatimukset ja näytöt toteutumisesta

- Tyypillinen haaste on organisaation kyky käsitellä standardien kokonaisuus sopivalla valikoinnilla
  - Toiminnallisen turvallisuuden asiantuntijoita tarvitaan

Turva-automaation suunnittelu ylhäältä alas



Toiminnallinen turvallisuus – uudet tuulet?

- Systems Engineering / Requirements Engineering ?
  - ISO/IEC/IEEE 15288:2015
  - ISO/IEC/IEEE 29148:2018
  - https://www.nasa.gov/connect/ebooks/nasa-systems-engineering-handbook
- Model-Based Systems Engineering (MBSE)?
  - https://www.incose.org/incose-member-resources/working-groups/transformational/mbse-initiative
- SafeScrum?
  - https://www.sintef.no/safescrum
- Safety differently / Safety II ?
  - https://safetydifferently.com/
- Systems Theoretic Process Analysis (STPA) / Systems Theoretic Accident Model and Processes (STAMP) ?
  - http://sunnyday.mit.edu/STAMP-publications.html

Systems and software engineering

- ISO/IEC/IEEE 15288:2015 – Systems and software engineering — System life cycle processes
- ISO/IEC/IEEE 12207:2017 – Systems and software engineering — Software life cycle processes
  - ISO/IEC/IEEE 15289:2019 – Systems and software engineering — Content of life-cycle information items (documentation)
  - ISO/IEC/IEEE 29148:2018 – Systems and software engineering — Life cycle processes — Requirements engineering
- Yleiset systems engineering-standardit sisältävät kattavan prosessien ja tukiprosessien määritelmäkehikon, jota voi soveltaa yrityskohtaisesti räätälöidyn kehitysprosessin määrittelyssä.
  - Työläs ja kallis räätälöinti ja käyttöönotto

Requirements engineering

- ISO 9000:2015 – design and development = set of processes that transform requirements for an object into more detailed requirements for that object

- ISO/IEC/IEEE 29148 requirement specifications
  - Business requirements specification (BRS)
  - Stakeholder requirements specification (StRS)
  - System requirements specification (SyRS)
  - Software requirements specification (SRS)

- *“When budgets are thin, timelines are tight, and scope is creeping, requirements documentation tends to be the first deliverable to go and the last deliverable to be considered.”*

- Vaatimuspohjainen suunnittelu versus dokumenttikeskeinen suunnittelu? (Requirement-based versus Document-centric)

Model-based systems engineering

- INCOSE defines MBSE as *“Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.”*

- Mallipohjainen suunnittelu versus dokumenttikeskeinen suunnittelu? (Model-based versus Document-centric)
  - Tietokantapohjaisuuteen siirtyminen voisi korostaa konfiguraation hallinnan tarpeita

Aiheen esille nosto

https://www.sintef.no/safescrum#/

- *Scrum, documentation and the IEC 61508-3:2010 software standard*
  - *IEC 61508 and several related standards for development of safety critical software has a strong focus on documentation, including planning, which shall show that all required activities have been performed. Agile development on the other hand, has as one of its explicit goals to reduce the amount of documentation and to mainly produce and maintain working software.*
  - *The problem created by the need to develop a large amount of documents when developing safety critical systems is, however, not a problem just for agile development – it has been identified as a problem for all development of safety critical software.* ***In some cases up to 50% of all project resources has been spent on activities related to the development, maintenance and administration of documents.*** *Thus, a way to reduce the amount of documentation will benefit all developers of safety critical systems.*

Sidney Dekker: Safety Differently

- *The second edition of a bestseller, Safety Differently: Human Factors for a New Era is a complete update of Ten Questions About Human Error: A New View of Human Factors and System Safety. Today, the unrelenting pace of technology change and growth of complexity calls for a different kind of safety thinking. Automation and new technologies have resulted in new roles, decisions, and vulnerabilities whilst practitioners are also faced with new levels of complexity, adaptation, and constraints. It is becoming increasingly apparent that conventional approaches to safety and human factors are not equipped to cope with these challenges and that a new era in safety is necessary.*

- *In addition to new material covering changes in the field during the past decade, the book takes a new approach to discussing safety. The previous edition looked critically at the answers human factors would typically provide and compared/contrasted them with current research and insights at that time. The edition explains how to turn safety from a bureaucratic accountability back into an ethical responsibility for those who do our dangerous work, and how to embrace the human factor not as a problem to control, but as a solution to harness.*

Engineering for Humans: A New Extension to STPA

- *Systems-Theoretic Accident Model and Processes (STAMP) is a new accident causality model developed by Nancy Leveson at the Massachusetts Institute of Technology. This model has inspired several new methods, from accident analyses like Causal Analysis based on STAMP (CAST) to hazard analyses like Systems-Theoretic Process Analysis (STPA). Unlike traditional methods, which are based on chain-of-events causality models and generally identify only component failures, STPA can be used to identify design flaws, component interactions, and human factors that contribute to accidents. Though STPA takes a more thoughtful approach to human error than traditional methods "requiring analysts to consider how system conditions may lead to errors" it does not provide extensive guidance for understanding why humans behave the way they do. Prior efforts have been made to add such guidance to STPA, but there has yet to emerge a widely accepted, easy-to-use method for examining human behavior using STPA.*

Yhteenveto

- SIL-normit ovat käytössä koeteltu menestystarina ja niiden purkaminen ei ole realistinen ajatus
  - Yksinkertaistettuja sovelluskohtaisia käytännesääntöjä voitaisiin kirjoittaa perustellen SIL-normien pohjalta
  - Moderneilla menetelmillä dokumentaation näpertely olisi mahdollista minimoida, mutta pilottien hinta on kallis
- Laajempi normitalkoo olisi monella toimialalla käynnistettävissä riskienhallinnan ja vaatimustenhallinnan menetelmien avulla
  - Vaatimusviidakon päällekkäisyyksien (”tårta på tårta”) purku
  - Käytännössä vaadittaisiin toimialakohtaisesti kaikkien toimijoiden yhteistyöfoorumeita ja –hankkeita
- Organisaatiotekijät, inhimilliset tekijät ja tietoturvallisuus linkittyvät toiminnallisen turvallisuuden elinkaareen