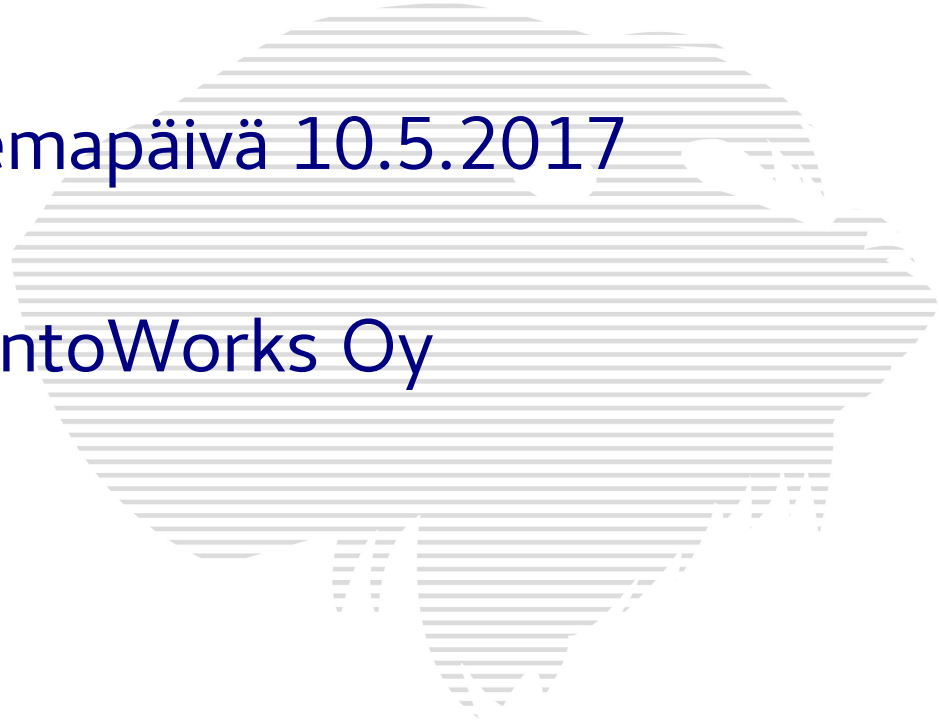
IntoWorks

Mikä tulevaisuudessa menikään pieleen?

Turva-automaation uudet vaatimukset ja automaation tietoturva,

Automaatioseuran teemapäivä 10.5.2017

Mika Koskela / IntoWorks Oy



IntoWorks

Into

IntoWorks

Mika Koskela
Partner
puh: 040 216 4132
email: mika.koskela@intoworks.fi

IntoWorks Oy
email: info@intoworks.fi
www.intoworks.fi

Johtava ajatus

- Peruskysymykset
  - Osaammeko tehdä oikeita asioita?
  - Jos osaamme, teemmekö silti?
    (Siis haluammeko?)
- Seuraavan ison ”tapahtuman” jälkeen joku kysyy näitä jokatapauksessa, ”**Miksi meni pieleen**?”
  - Tässä esityksessä pari täkyä tulevaisuuden rootcause pohdintoihin

IntoWorks

Osaaminen

- Hypoteesi: Automaation tietoturvallisuuden taso on parantunut merkittävästi
  - Tietoisuus on loikannut eteenpäin
  - Standardeja ja kirjallisuutta löytyy
  - Koulutusta löytyy sekä teoriamielessä + hand-on:nina
  - Tekijöitä löytyy sekä palveluina että työmarkkinoilta
  - Tietoisuus: Totta. Kaikki osaavat ainakin pelätä (post-stuxnet era)
  - Tosi on.
  - Vapailla markkinoilla tarjonta runsastunut, ja taitoja opiskellaan myös oppilaitoksissa
  - Tilanne koko ajan parantumassa
- Kaiken kaikkiaan näyttää hyvältä.

IntoWorks

Osaaminen

- Hypoteesi: Automaation tietoturvallisuuden taso on parantunut merkittävästi
  - Tietoisuus on loikannut eteenpäin
  - Standardeja ja kirjallisuutta löytyy
  - Koulutusta löytyy sekä teoriamielessä + hand-on:nina
  - Tekijöitä löytyy sekä palveluina että työmarkkinoilta
  - Tietoisuus: Totta. Kaikki osaavat pelätä. (post-stuxnet era) Osataanko toimia?
  - Standardeja ja kirjallisuutta löytyy. Totta. Suurin osa opettaa riskianalyysilähtöistä epistolaa.
  - Koulutus: keihäänkärkiosaaminen kyllä. Monessako oppilaitoksessa opetetaan soveltavan riskianalyysin tekemistä?
  - Tilanne koko ajan parantumassa
- Kaiken kaikkiaan näyttää yhä hyvältä, <u>etenkin jos uhkataso on pysynyt samana</u>.

Toimintaympäristön kehitys

- IoI: Internet of Idiots
  - Tästä ei tarvinne enempää sanoa
- Painopisteen siirtyminen (isojen resurssien) valtiolliseen toimintaan
  - Harmaan alueen tummempi pää: yhteiskunnan normaalitoimintojen, tuotannon, logistiikan ja perusinfran häirintä
  - ”Valtiolliskaupallisidealistiset toimijat”
- Vaikeudet saada selkeää tilannekuvaa (ovatko oireet bugeja vai jotain muuta, epätietoisuus ja sen sietäminen)
- *With today's attack sophistication, it is inevitable hackers will get in, the issue is all about containing and mitigating*
  - Gregory Hale, isssource.com, 14.9.2016

Motivaatio on parantunut

- Muutamia retorisia kysymyksiä:
  - Moraali on parantunut?
  - Tiedon kulku on parantunut?
  - Kuka kaupallinen toimittaja joka tunnustaa että tuotteidensa tietoturvallisuudessa olisi parantamisen varaa?
- Taloudellista toimintaa ohjaa raha ja sen virtaaminen
  - Vaihtoehto A: optimoidaan asiakkaan etu ja turvallisuustaso
  - Vaihtoehto B: ALACA/ALARA
    (As Low As Contract Allows,
    turvallisuuskriittisille As Low As Regulator Allows)
- Oikeastaan: perusrajoitteille ei voida mitään

IntoWorks

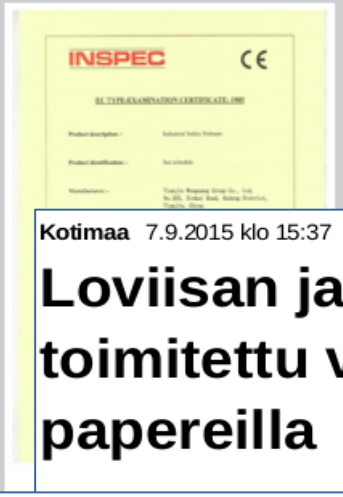
Etiikasta

Päästöhuijaus 7.3. 19:42

EU yllyttää kansallisia viranomaisia vaatimaan korvauksia Volkswagenilta, Suomen kuluttajavirasto nihkeänä – ”Ei vielä tarvetta oikeustoimille”

EU yrittää yhdistää kansallisten kuluttajaviranomaisten voimat Volkswagenia vastaan, jotta myös eurooppalaiskuluttajat saisivat korvauksia.

Examples of Fake Safety Certificates http://www.bsif.co.uk/en-149



Kotimaa 7.9.2015 klo 15:37 | päivitetty 7.9.2015 klo 16:05

Loviisan ja Olkiluodon ydinvoimaloihin toimitettu venttiilejä väärennetyillä papereilla

venttiilien väärennetyt materiaalien
kentäneet ydinvoimaloiden turvallisuutta.

digitoday

Hakkerit päihittivät Volkswagenin – joka yritti vaientaa heidät

17.8.2015 13:30 — Bloomberg–Digitoday

Volkswagen taisteli kaksi vuotta salatakseen kolmen tietoturvatutkijan löytämän ongelman autojen varkaussuojassa.

IntoWorks

Esimerkki: Riskianalyysiorientoituneisuus

- State-of-the-art nojaa riskianalyyseihin
  - Lähestymistapa: suojattavat kohteet -> riskit -> riskit hallintaan kontrolleilla
    - ISO 27001: *The information security management system preserves the confidentiality, integrity and availability of information **by applying a risk management process** and gives confidence to interested parties that risks are adequately managed.*
    - IEC 62443-1-1: *Uhkien ja riskien arviointiprosessissa suojattavat **kohteet ovat alttiina riskeille**. Näitä **riskejä vuorostaan minimoidaan** käyttämällä vastatoimenpiteitä, joita sovelletaan erilaisten uhkien käyttämien tai hyödyntämien haavoittuvuuksien käsittelyyn.*
- *Can risk be effectively managed? The sober reality is that in respect to the cyber security of critical infrastructure, there is no empirical evidence that a risk-based approach, despite its near decade of practice, has had any success.*
  - (Langner & Pederson, 2013: Bound to Fail: Why Cyber Security Risk Cannot Simply Be ”Managed” Away)
- Käytännössä: Antaako (kalliin) virhekäsityksen hallinnasta?
  - Tyypillinen virhe: pyöritellään riskianalyysin tuloksia liian korkealla tarkkuustasolla riskien arviointiin liittyvään epävarmuustasoon nähden
  - Kalkkunaharha (aina läsnä, myös safety-puolella)
  - Domain-osaamisen aliarviointi: Ajatellaan että määrämuotoisella riskiarviointiprosessilla voidaan korvata asiantuntijuutta
  - Panos-tuottosuhde?

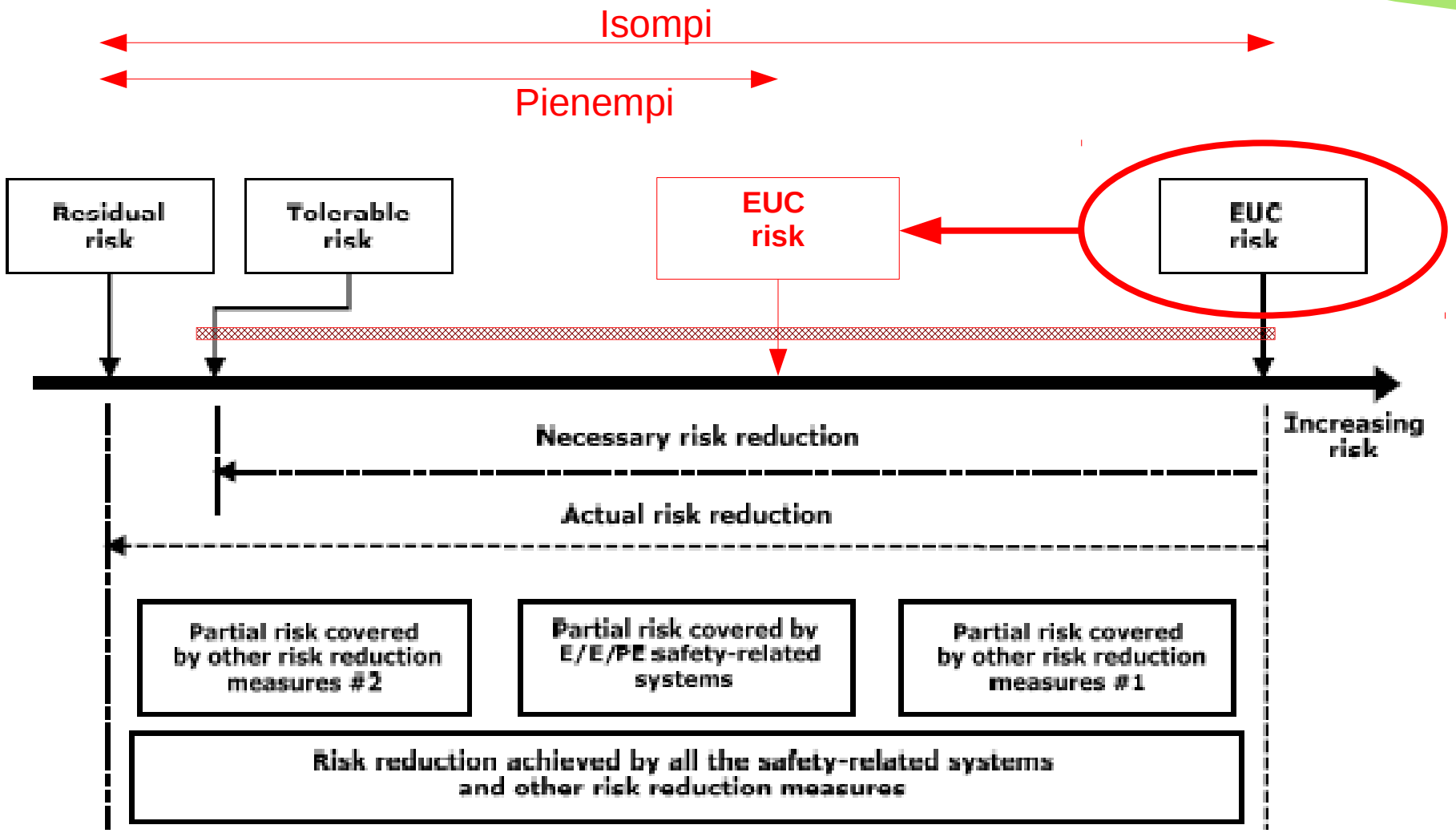
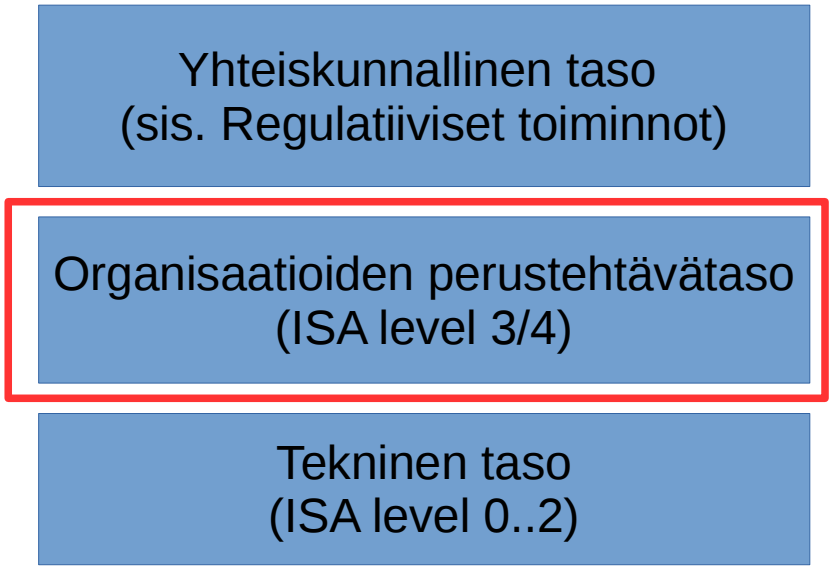


Figure A.1 – Risk reduction – general concepts (low demand mode of operation)

IntoWorks

Missä pitäisi onnistua

- Resilienssi (iskunkestävyys): "the ability [of a system] to cope with change"
  - Systeeminen käsite, jossa systeemi tarkoittaa tyypillisesti jotain laajempaa kokonaisuutta kuin yksittäistä automaatiojärjestelmää
- Filosofisesti avain on riippumattomuudessa ja tähän liittyvässä todennäköisyydessä P(A & B) = P(A)P(B)
- Vanha kunnon ”Ei kaikkia munia samaan koriin” -ajattelu
  - Panos-tuotto mielessä kyse on sijoittaakko reduntanttiseen toimintaan (jolla varmistetaan riippumatomuus) vai optimoidaanko varsinaisen järjestelmän suojaa/sietokykyä
- Haasteena on, että oikeat ratkaisut ovat joskus kaupallisesti väärällä tasolla. Automaatiotoimittajalle alimman tason ”lelukauppa” on helppoa, kun taas keskitasolla toimiminen vaatii kohdeorganisaatioilta kokonaisnäkemystä ja usein myös vahvaa verkostoitumista.



Kremlin returns to typewriters to avoid computer leaks

The Kremlin is returning to typewriters in an attempt to avoid damaging leaks from computer hardware, it has been claimed.

German-made Triumph Adler Twen 180 typewriters were popular in the late '80s and early '90s

By Chris Irvine, Tom Parfitt in Moscow and agencies
2:19PM BST 11 Jul 2013

Russia

The Telegraph, 11.7.2013

IntoWorks

Kiitos!