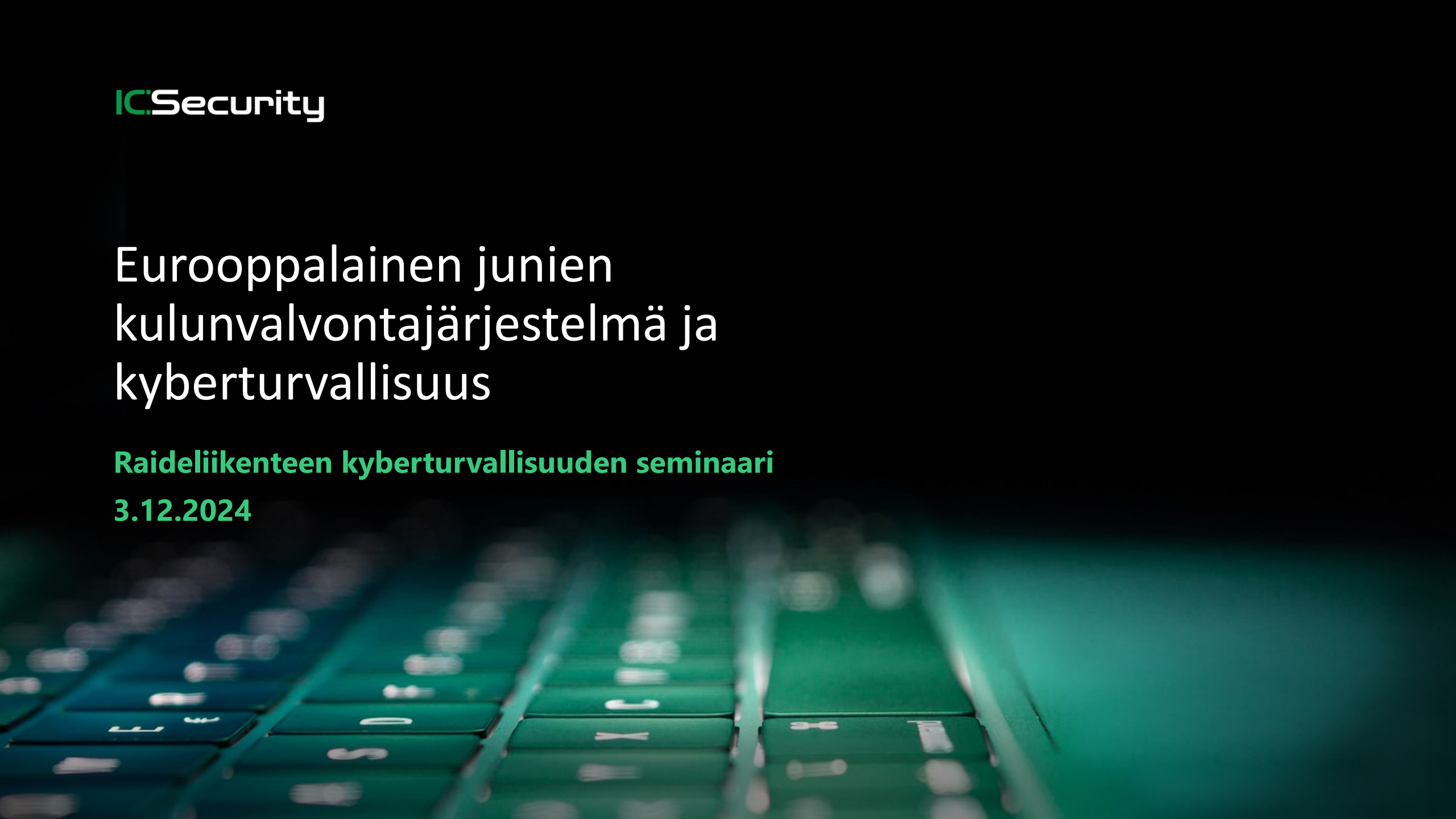
IC:Security

Eurooppalainen junien kulunvalvontajärjestelmä ja kyberturvallisuus

Raideliikenteen kyberturvallisuuden seminaari

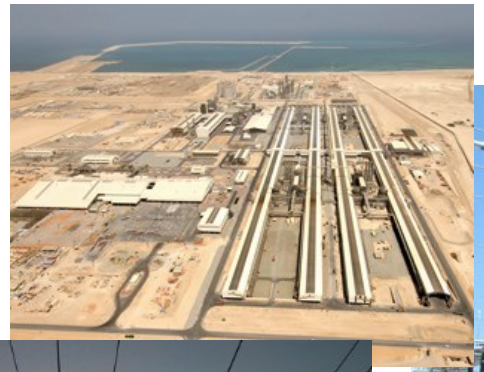
3.12.2024



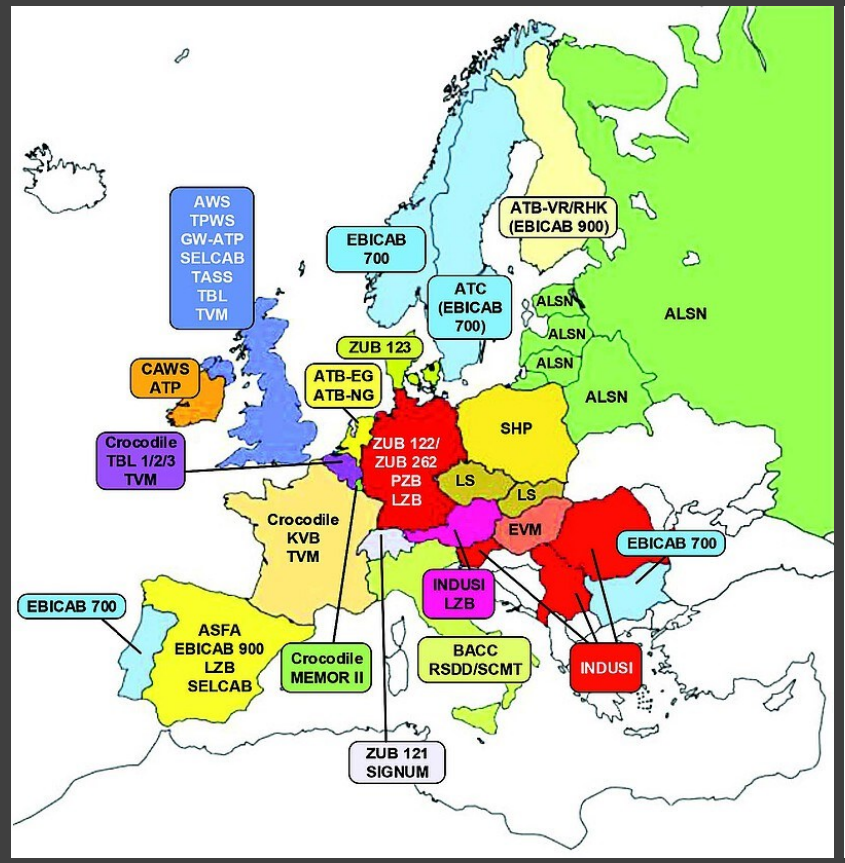
Minä

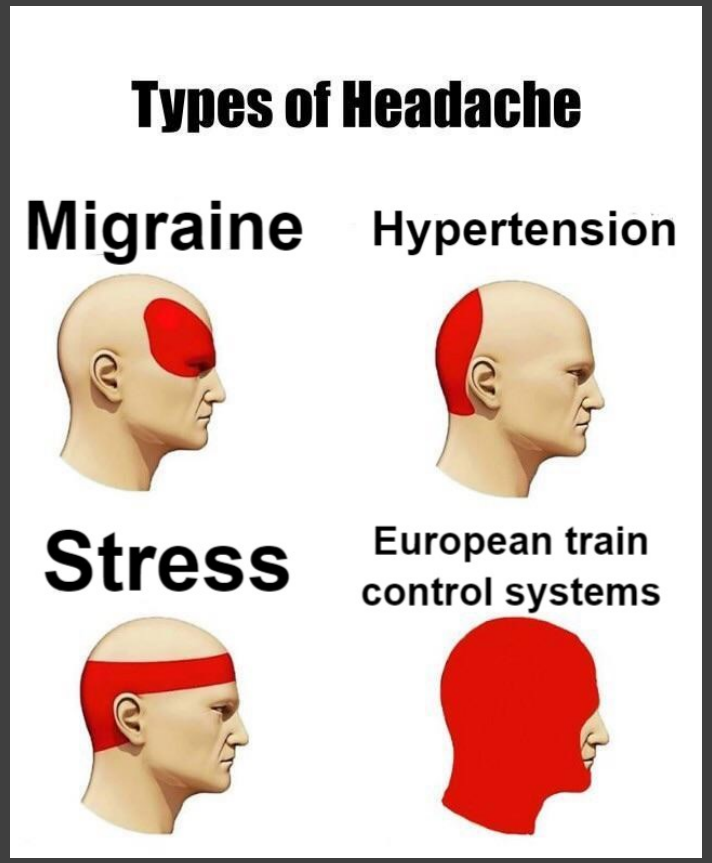
- Opinnot: Teknillinen korkeakoulu, tietotekniikka (nyk. Aalto)
- KPMG 2007-2018
- Yrittäjä 2019-

Kokemus



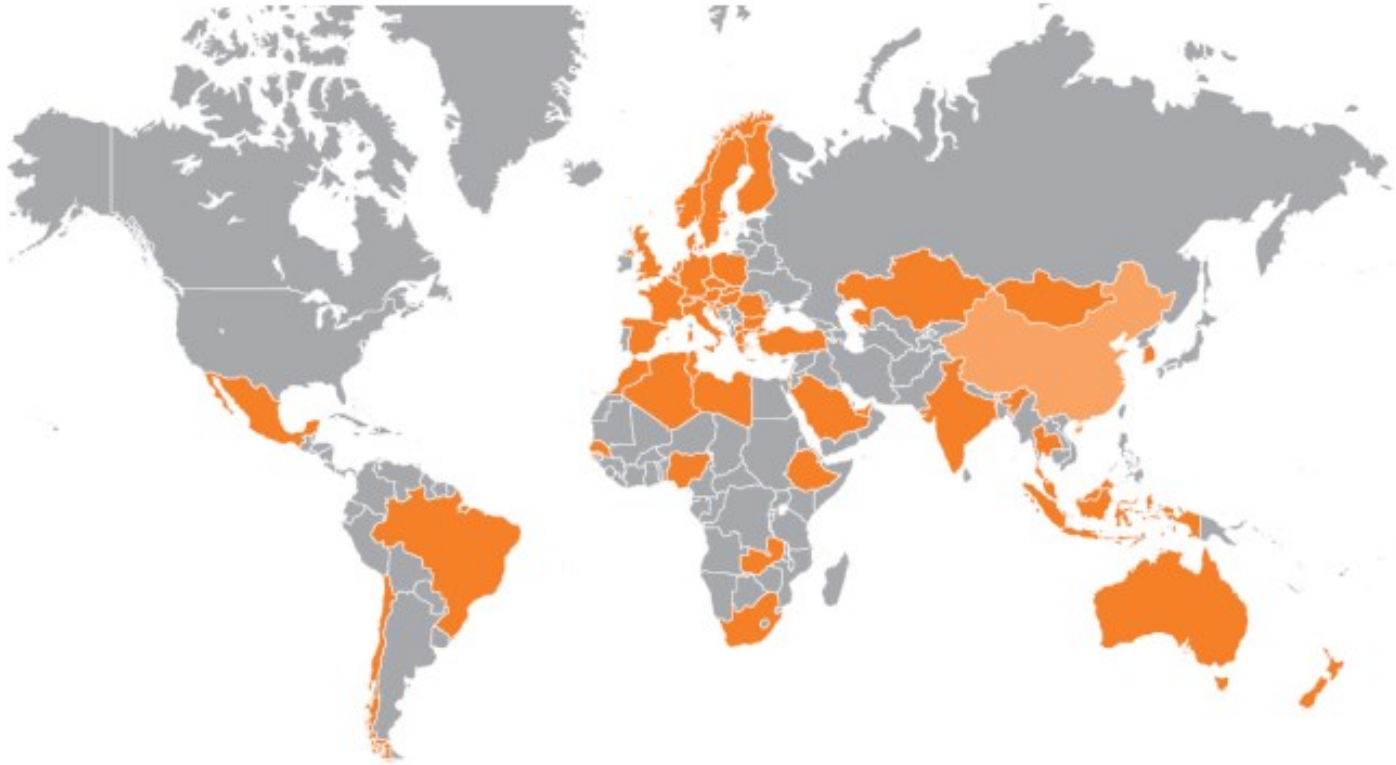
Rautatieympäristö


AWS
TPWS
GW-ATP
SELCAB
TASS
TBL
TVM
EBICAB 700
ATB-VR/RHK (EBICAB 900)
ATC (EBICAB 700)
ALSN
ALSN
ALSN
ALSN
ALSN
ZUB 123
CAWS ATP
ATB-EG
ATB-NG
SHP
Crocodile TBL 1/2/3 TVM
ZUB 122/ ZUB 262 PZB LZB
LS
LS
EVM
EBICAB 700
Crocodile KVB TVM
INDUSI LZB
EBICAB 700
ASFA EBICAB 900 LZB SELCAB
Crocodile MEMOR II
BACC RSDD/SCMT
INDUSI
ZUB 121 SIGNUM


Types of Headache
Migraine
Hypertension
Stress
European train control systems

Ennen

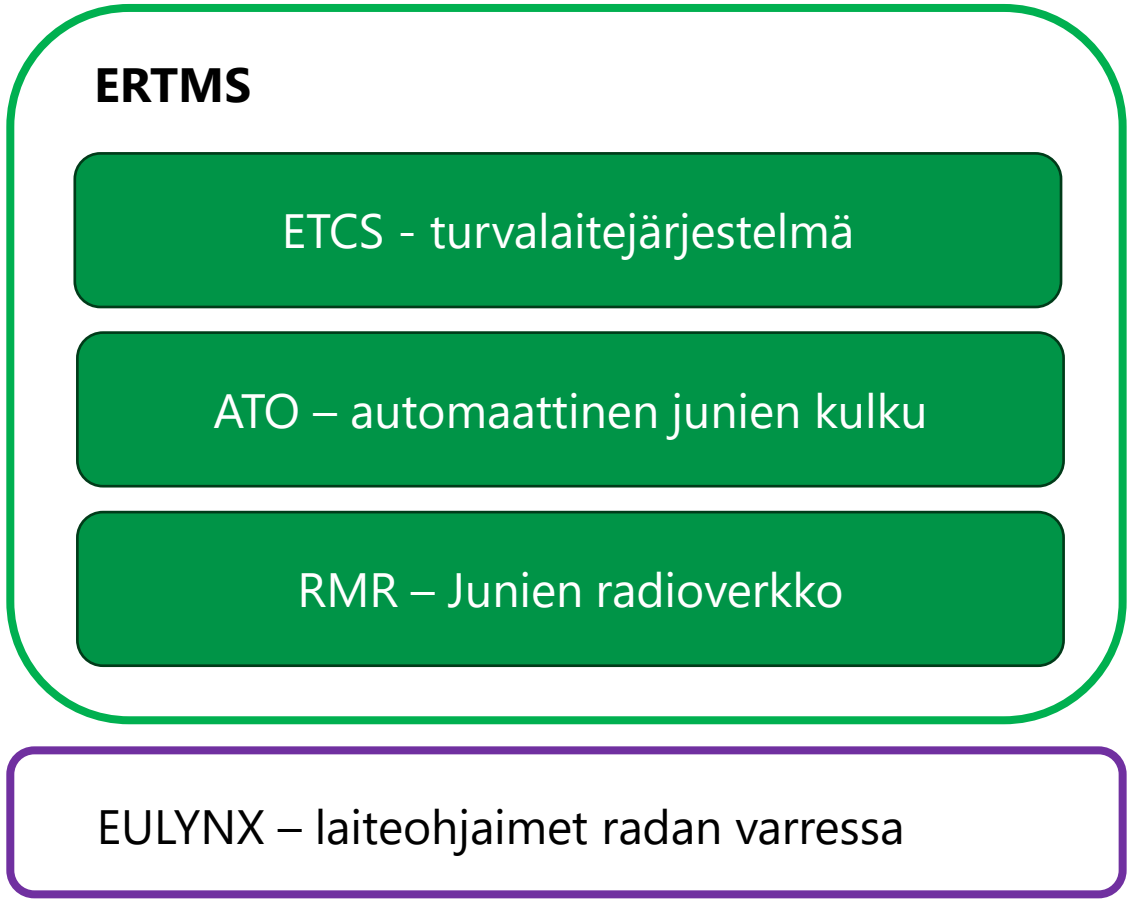
Jälkeen



Standardit ja määrittelyt

Eurooppalaiset standardit

- European Rail Traffic Management System
  - European Train Control System
  - Automatic Train Operation
  - Railway Mobile Radio
  - (EULYNX)



IC Security

ETCS tasot

- ETCS
  - Turvallisuusjärjestelmä, joka pakottaa yhteensopivuuteen maiden välillä
  - Estää junia ajamasta ylinopeutta tai ajolupaa pidemmälle
- ETCS-tasot
  - Taso 1 – Junat paikallistetaan radan infrastruktuurilla. Opastimet radan varressa.
  - Taso 2 – Junat paikallistetaan radan infrastruktuurilla. Ajolupa saadaan radioverkon yli. Ei opastimia.
  - Taso 2 + HDT (Hybrid Train Detection) – Junat paikallistavat itsensä ja raportoivat sen mobiiliverkon yli. Junien eheyden valvonta junassa. Ajolupa kuten tasolla 2.

IC Security

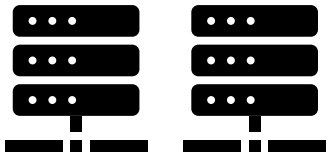
Arkkitehtuuri – yksinkertaistettu

Moni-
kanava-
reititin

ETCS-
veturilaite +
kuljettajan
käyttöliittymä

Junakalusto

Future
Railway
Mobile
Comms
System



Radio-
suojastus-
keskus

Asetinlaite

Keskitetty turvalaitejärjestelmä

Liikenteen-
ohjaus-
järjestelmä

Liikenteen-
ohjaajat

Liikenteenohjaus

IC Security

ERTMS/ETCS uutuuksia

- Radiosuojastuskeskus eli radio block center (RBC)
- Monikanavareititin junassa
- 5G-pohjainen radioverkko FRMCS
  - …määrittelyt vieläkin kesken
  - Euroopassa vielä GSM-R käytössä
- Uusi arkkitehtuuri
  - Asetinlaitteet voidaan keskittää
  - Mahdollistaa myös hajautuksen useampaan sijaintiin (silti keskitettynä)
- ETCS-veturilaite ja kuljettajan käyttöliittymä

IC Security

Todellisuus

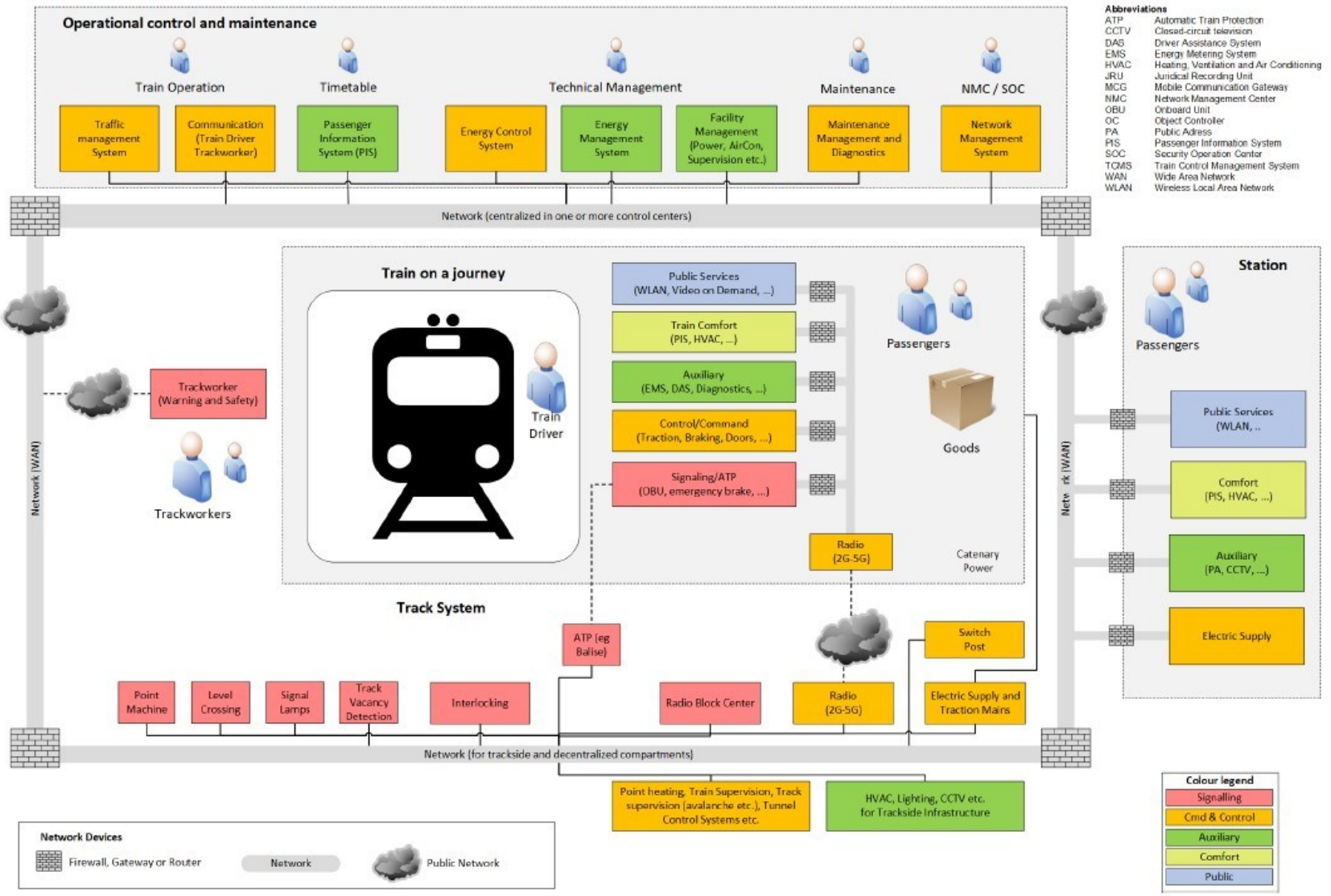
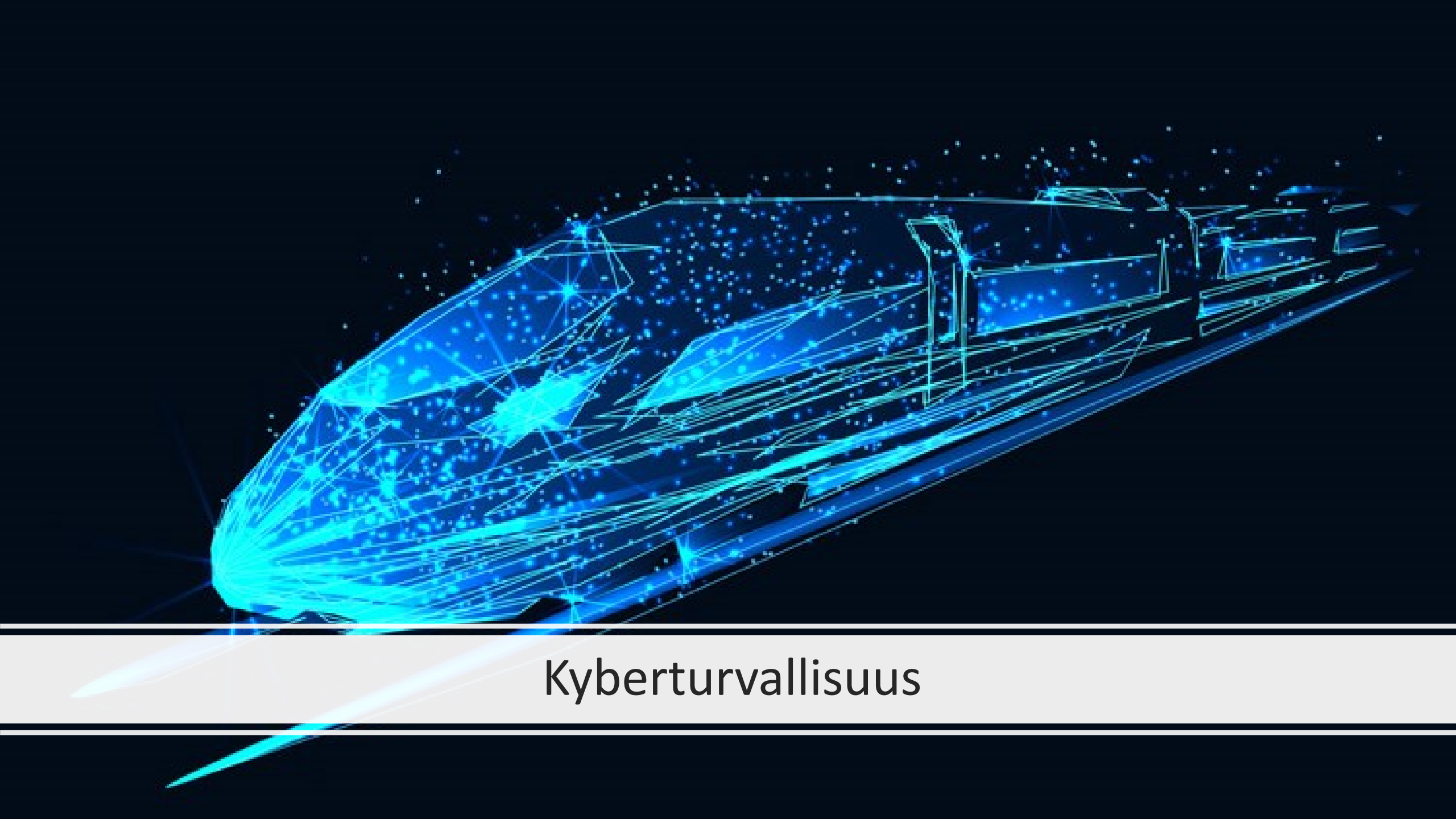


Figure 3 — Railway physical architecture model (example)

Suomen Digirata-projekti

- Tavoitteena lisätä radan kapasiteettia, luotettavuutta ja turvallisuutta
- Suomi menee suoraan ETCS tasolle 2
- Aluksi toteutetaan kansallinen radioverkkoratkaisu
  - Käyttää kaupallisia radioverkkoja
  - Suomessa ei ole GSM-R:ää
  - FRMCS määrittelyt eivät ole valmiina; valmistuminen ja tarjonta markkinoilla epävarmaa
- Tavoitteena ETCS taso 2 + HDT ja puoliautomaattiset junat
- Ensimmäisen radan teknologia ja toteutus on kilpailutettu ja rakentaminen on alkanut, kaupallisessa liikenteessä 2028

IC Security



Kyberturvallisuus

Kyberturvallisuuden haasteet rautatieympäristössä

- Hajautettu rakenne laajalle maantieteelliselle alueelle
- Radioverkkojen käytössä on paljon riskejä
  - Kaupallisten verkkojen käyttö lisää joitakin näistä
- Junien paikantamisessa on riskejä
- ETCS:n ja muiden teknologioiden määrittelyissä on riskejä
  - 3DES, MD4 …
  - Salausta ei ole määritelty junien ajolupaviesteille, ainoastaan allekirjoitukset
    - Hätäviestit eivät vaadi edes allekirjoitusta
- Puutteellinen kyberosaaminen yhdistettynä rautatieosaamiseen

IC Security

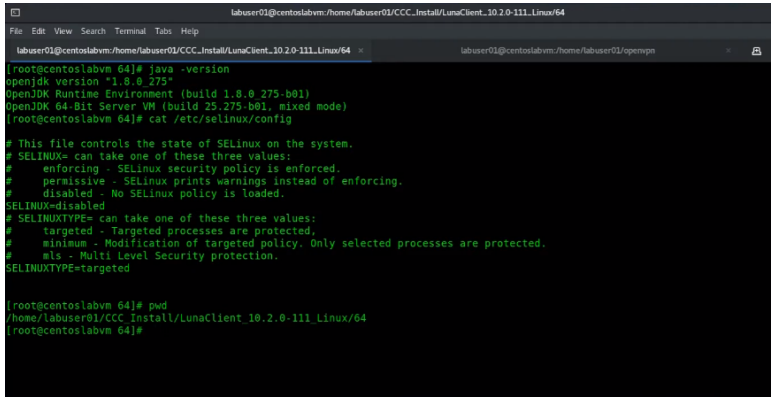
Ratkaisut

- Turvallisen kokonaisjärjestelmän suunnittelu
- Standardit ja ohjeet
  - 62443-sarja
  - TS 50701 eli 62443-3-3 opas rautateille
  - Edellistä laajentava, tuleva IEC 63452
  - Standardit kertovat paljon, MITÄ pitää tehdä, mutta eivät välttämättä MITEN
- Sovelletaan IT:n tietoturvaa automaatioympäristössä
  - Turvallinen arkkitehtuuri
  - (Passiivinen) tietoturvan valvonta
  - Haittaohjelmien torjunta ja erikseen hyväksytyt ohjelmistot
  - Keskitetty pääsynhallinta
  - Verkkoliikenteen salaus

IC Security

Vanha vs. uusi

vs.

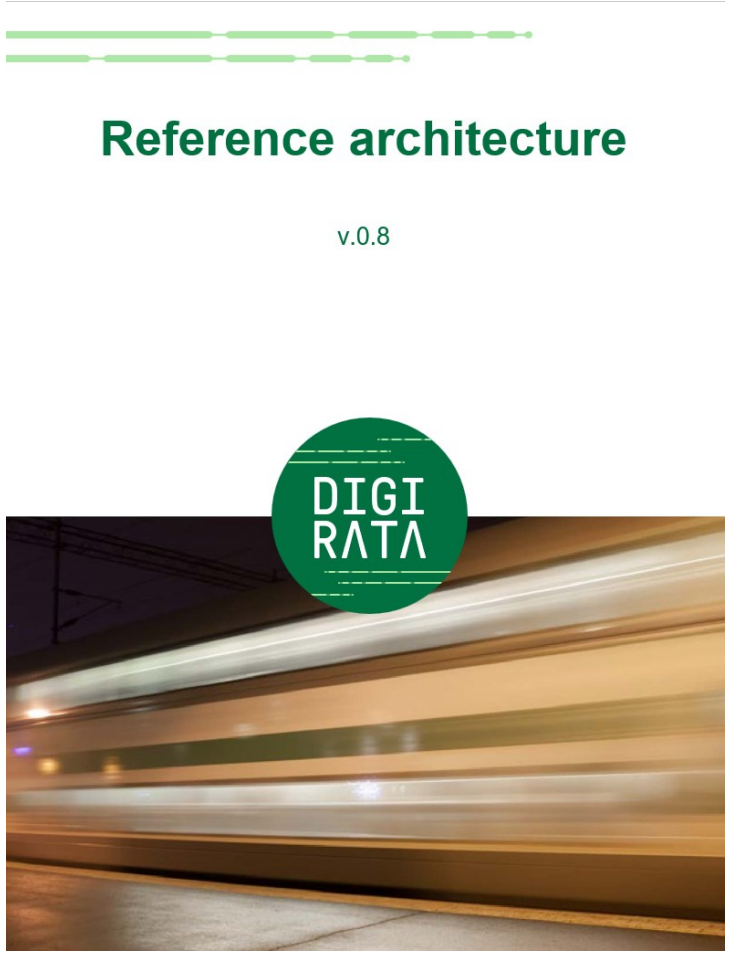


Siemens Westrace mk. II

Joku Thalesin ratkaisu, joka pyörii CentOS:llä

IC Security

Esimerkki – Puolustettava arkkitehtuuri



- Paras tapa estää hyökkäykset
- Suunniteltava ja ylläpidettävä
  - Ihmiset ja prosessit tärkeitä ylläpidon kannalta
- Referenssiarkkitehtuuri järjestelmätoimittajille
- Uusien uhkien ja haavoittuvuuksien ymmärtäminen
  - Digiradan uhkaympäristön dokumentointi

Esimerkki – Verkon tietoturvan valvonta

- Pääasiassa passiivista – ei skannausta
  - “Skannaus” on OK, jos se tapahtuu normaalien rajapintojen kautta
- Ymmärrettävä rautatiespesifisiä protokollia ja laitteita
- Ei saa olla intruusiivistä
  - Turvallisuus > tietoturva
- Kuinka koko verkko voidaan kattaa?
  - Entä junat?
- Integraatio SIEMin ja SOCin kanssa?
  - Voiko SOC ratkaista hälytykset? Jos ei, kuka muu?

IC Security

Esimerkki – Kuinka junat voivat luottaa käskyihin?

- Ongelma: Kuinka juna voi tietää, että käskyn lähetti siihen oikeutettu taho?
- Ratkaisu: Avaintenhallintajärjestelmä
  - Jokaisella laitteella (juna / radan varren turvalaite) on avain, jolla viestit allekirjoitetaan
- Ongelma: Kuinka avaimia hallitaan järkevästi?
- Ratkaisu: Verkkopohjainen avaintenhallintajärjestelmä
- Ongelma: Kuinka avaimet pidetään salassa siirron ajan?
- Ratkaisu: Käytetään TLS:ää
- Ongelma: Kuinka varmenteita hallitaan?
- Ratkaisu: Käytetään PKI:tä
- ...kryptografiaa aina alas asti!

IC Security

IC:Security

Kysymyksiä?

Kiitos!

- IC Security Oy
- Antti Alestalo
- etunimi.sukunimi@icsecurity.fi

- www.icsecurity.fi