Funded by
the European Union
NextGenerationEU

Onboard cyber security seminar

12.3.2024

DIGI RAIL

Funded by
the European Union
NextGenerationEU

Seminaarin sisältö

- **ERTMS raidekyberturvallisuuden perusteita** (20min, Juhana Yrjölä)
  Esityksessä käydään läpi ERTMS/ETCS –järjestelmän kyberturvallisuuden perusteita, jotka vaikuttavat erityisesti raideoperaattoreihin tulevaisuuden Digiradalla toimiessa.

- **Digiradan uhkaympäristö kaluston näkökulmasta** (20min, Antti Alestalo ja Samuli Korpimäki) Esityksessä käydään läpi lyhyesti Digiradan luomaa uhkaympäristön kartoitusta ja miten siellä olevat asiat suhtautuvat kalustoon.

- **Tanskan kokemukset Onboard-asennuksista** (20min, Martin Allesen)
  Onboard yksikköjen tekninen yleiskatsaus, onboard hyväksyntäprosessit ja ERA One Stop Shop (OSS), mukaan lukien kyberturvallisuus. Esitys on englanninkielinen.

- **Kysymyksiä ja vastauksia -osio** (30min)

DIGI RAIL

Funded by
the European Union
NextGenerationEU

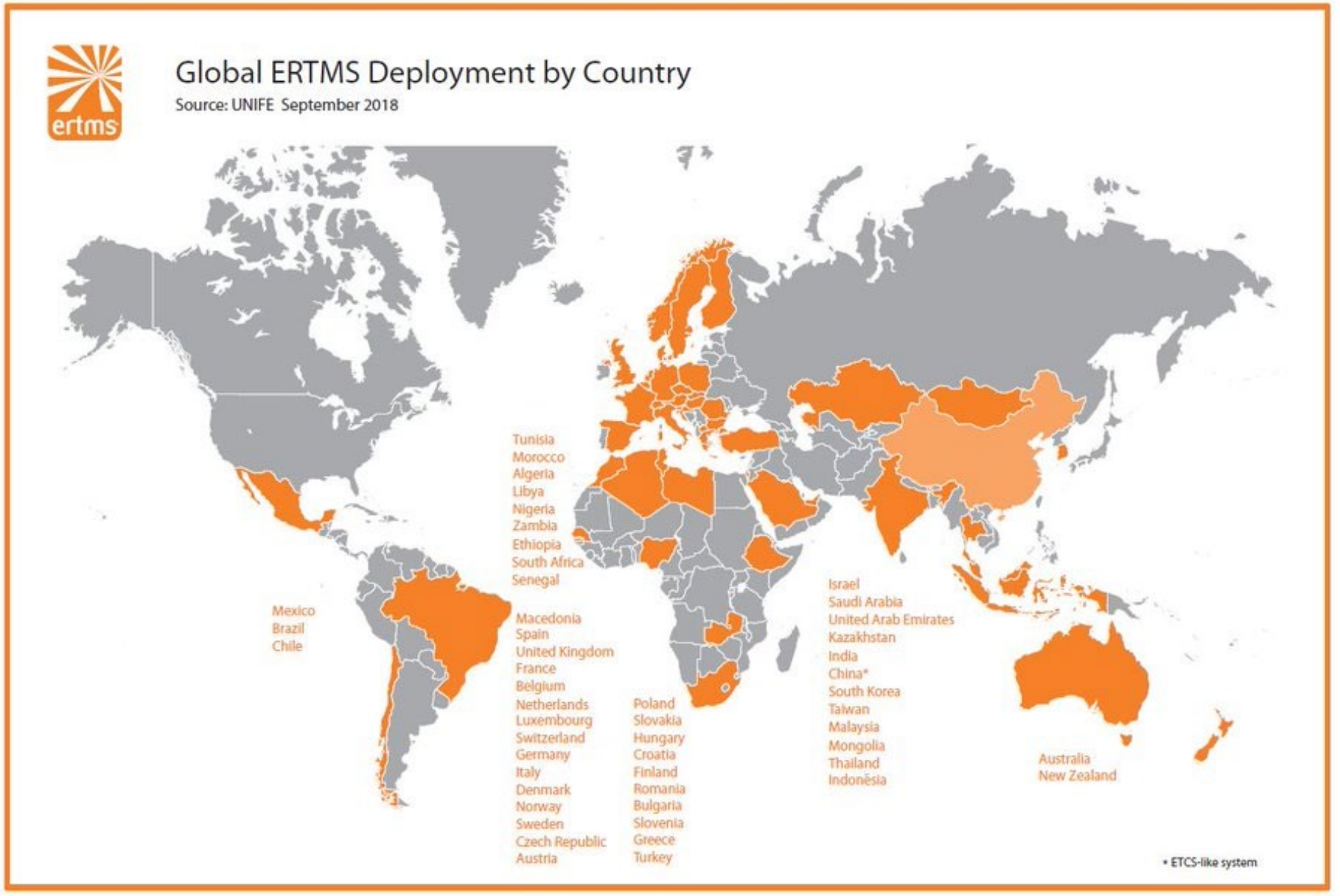
Onboard cyber security training: Rail cyber basics

Juhana Yrjölä
12.3.2024

DIGI RAIL

About ERTMS and ETCS

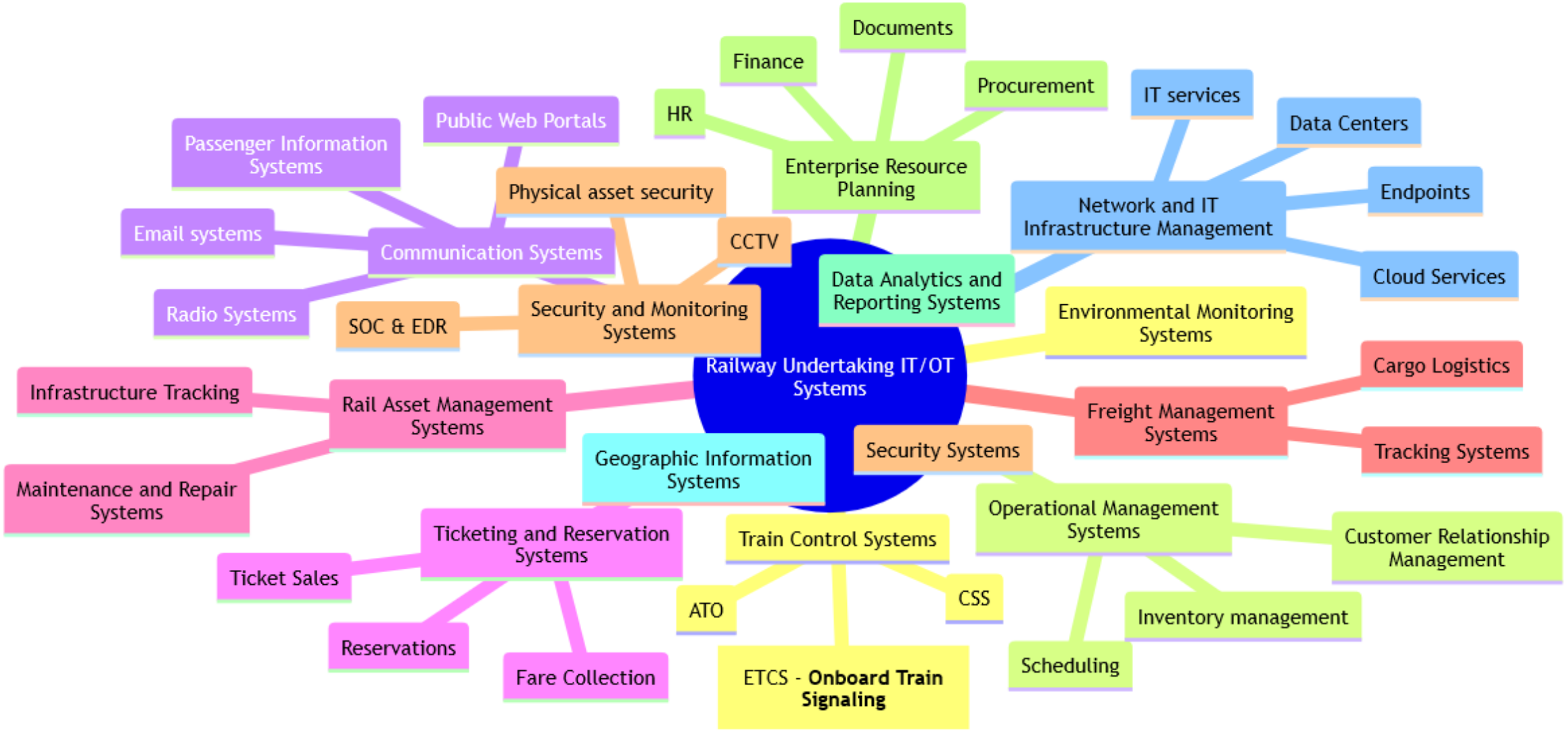
Funded by
the European Union
NextGenerationEU



DIGI RAIL

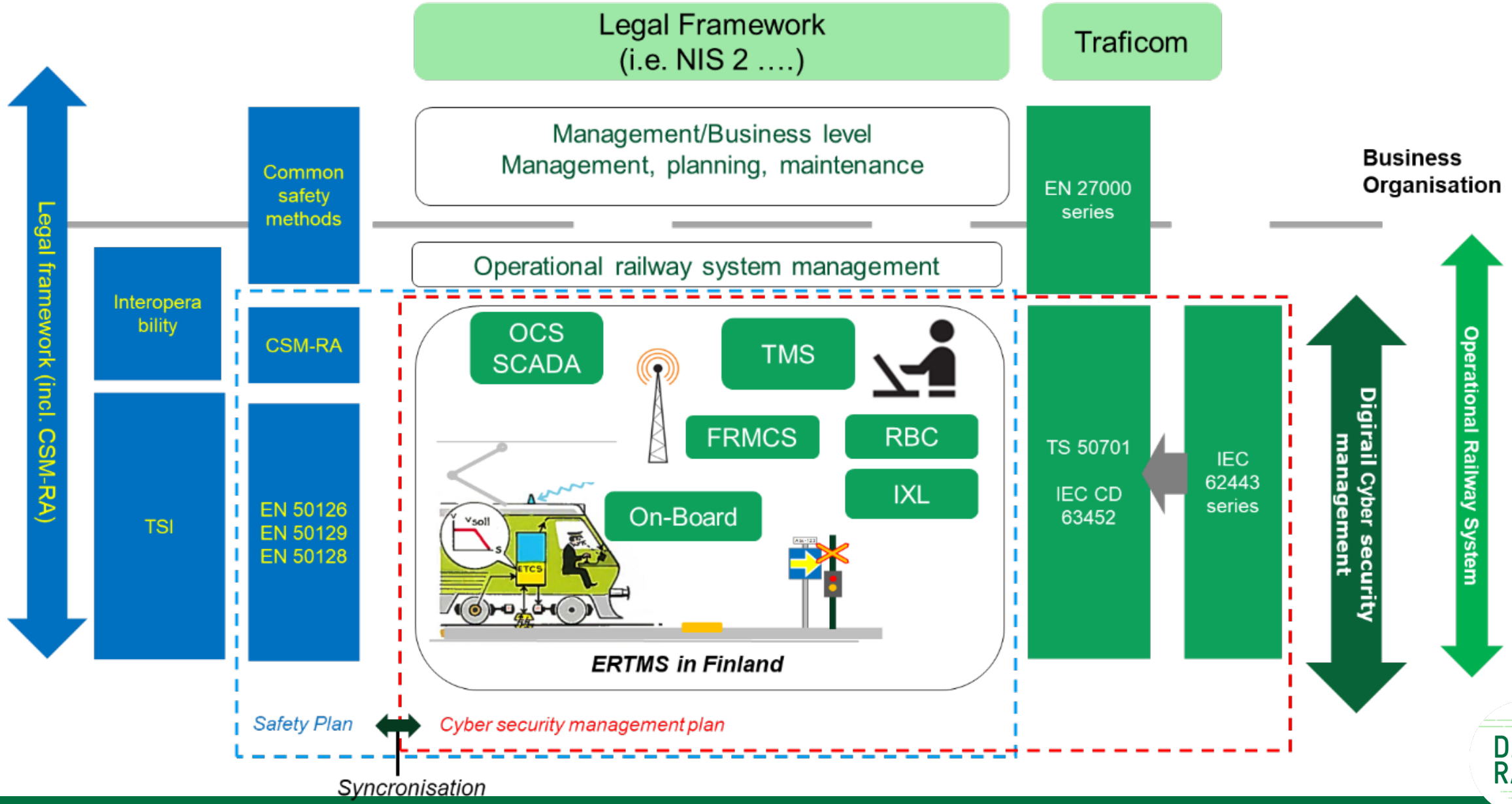
Rail organization cyber attack surface

Funded by the European Union



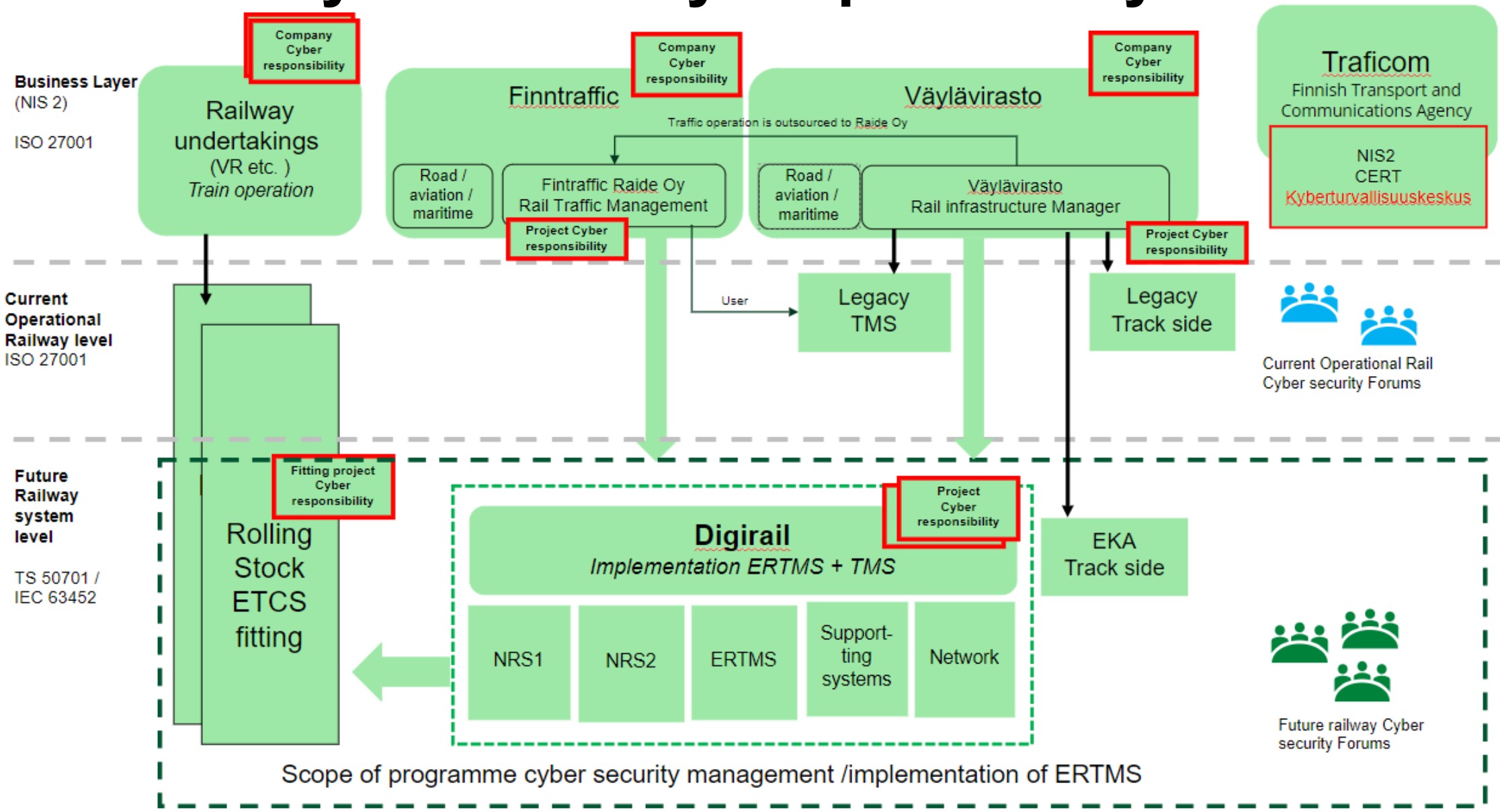
*Chat GPTs view

Funded by
the European Union
NextGenerationEU



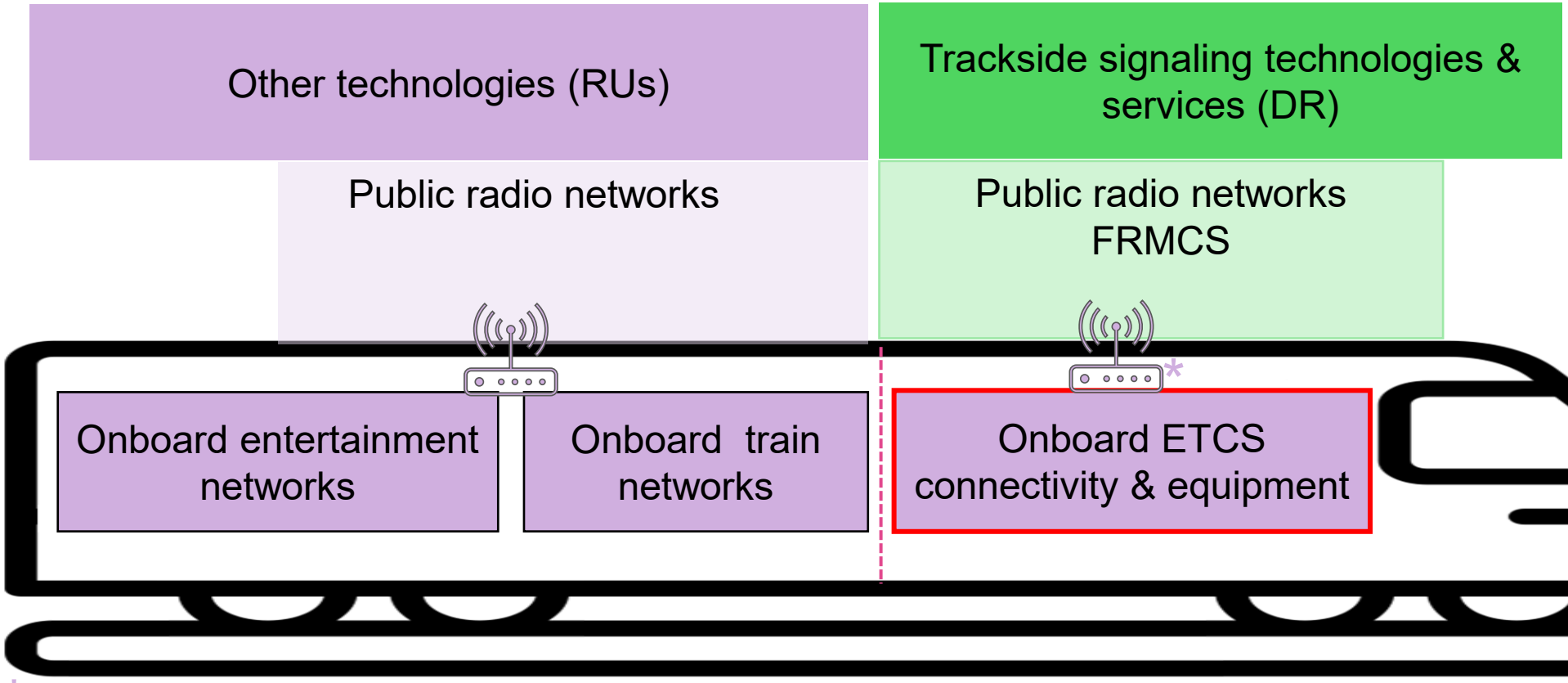
Shared cyber security responsibility model

Funded by the European Union
NextGenerationEU



Responsibilities of operational cyber security

Funded by the European Union
NextGenerationEU



Responsibilty:

- Digirail (DR)
- Mobile network operators based on contracts (DR)
- Mobile network operators based on contracts (RUs)
- Railway operators (RUs) or service providers

* FRMCS 4/5G router is responsibility of the owner RU. Digirail project will provide technical guidance on cyber protections/configuration of router.

NRS1 cyber requirements

Funded by the European Union
NextGenerationEU

ID	Area	Comments
1.	Traficom & ERA guidelines	Currently there are no known applicable guidelines
2.	Proper segmentation/firewalling	
3.	Hardening	
4.	Restricted access with least priviledges	Physical & logical
5.	Patching	
6.	Logging	
7.	Incident response	
8.	Change management	
9.	Remote connections	
10.	Audit	

Note that exact technical requirements depend on the business goals, needs, and risk appetite. Also note that above requirements are extra requirements on top of ERA/EU.

DIGI RAIL

DIGI RAIL

Digirata – Kaluston uhkaympäristö

Antti Alestalo ja Samuli Korpimäki

Funded by the European Union
NextGenerationEU

Funded by
the European Union
NextGenerationEU

Sisältö

- Uhkaympäristön esittely
- Uhkien torjuminen
- Kaluston omistajien näkökulma
- Yksinkertaistettu arkkitehtuuri

- Kalustoon liittyvät uhat
  - Palvelunestohyökkäykset
  - Verkon häirintä
  - Haittaohjelmat
  - Toimitusketju

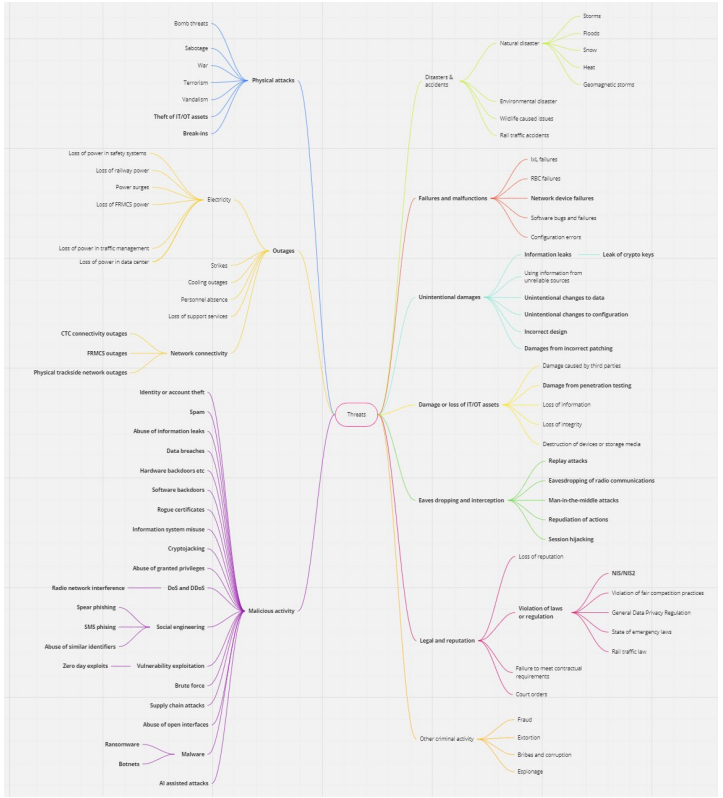
Funded by
the European Union
NextGenerationEU

Uhkaympäristö

Funded by
the European Union
NextGenerationEU

Uhkaympäristö

- Digiradan uhkaympäristö kartoitettu 2022
  - Päivitetty 2023
- Pyrkii kattamaan kaikki rautatieympäristöjen uhat kyberin näkökulmasta
  - Kyber ei välttämättä vastaa kaikkien uhkien torjunnasta
- Oheisen kuvan lisäksi uhat on listattu myös erillisessä excel-tiedostossa, jossa enemmän yksityiskohtia

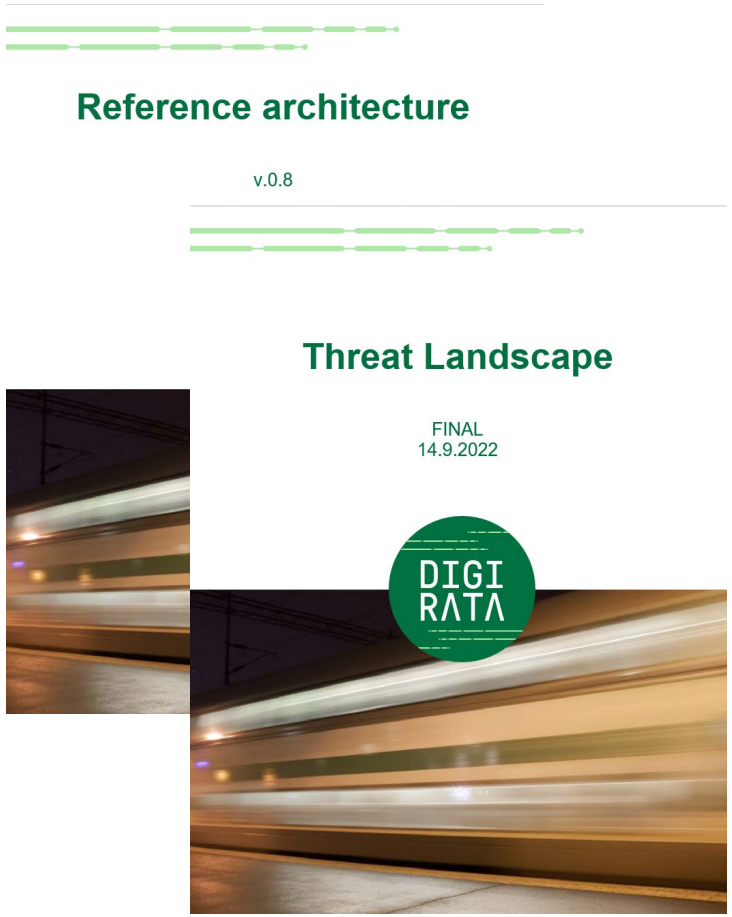


Funded by
the European Union
NextGenerationEU

Uhkien torjuminen

- Digiradassa on tehty uhkien torjuntaa mm. seuraavilla toimilla:
  1) Järjestelmäarkkitehtuurin määrittely
     - Kuvattu vyöhykkeet ja yhteydet
     - Kokonaisarkkitehtuurin kuvaus
  2) Kyberturvallisuuden vaatimukset toimittajille
  3) Verkon tietoturvan valvonta
  4) Haavoittuvuuksien hallinta
  5) Muutoksen hallinta
  6) Etäyhteyksien hallinta ja vahva tunnistaminen
  7) Toimittajien hallinta
  8) Poikkeamienhallinnan suunnitelma

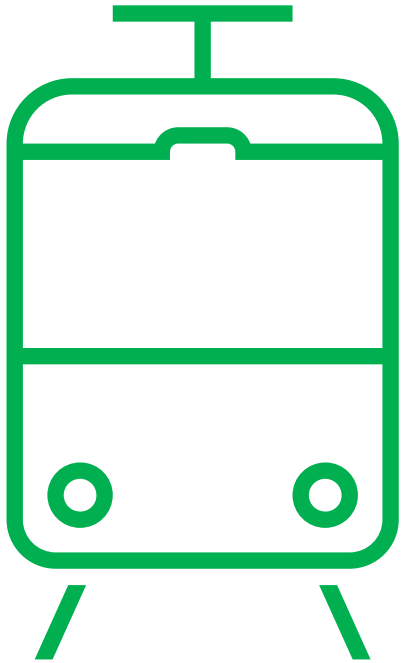
- Rataverkon haltija vastaa kokonaisuuden tietoturvasta



Funded by
the European Union
NextGenerationEU

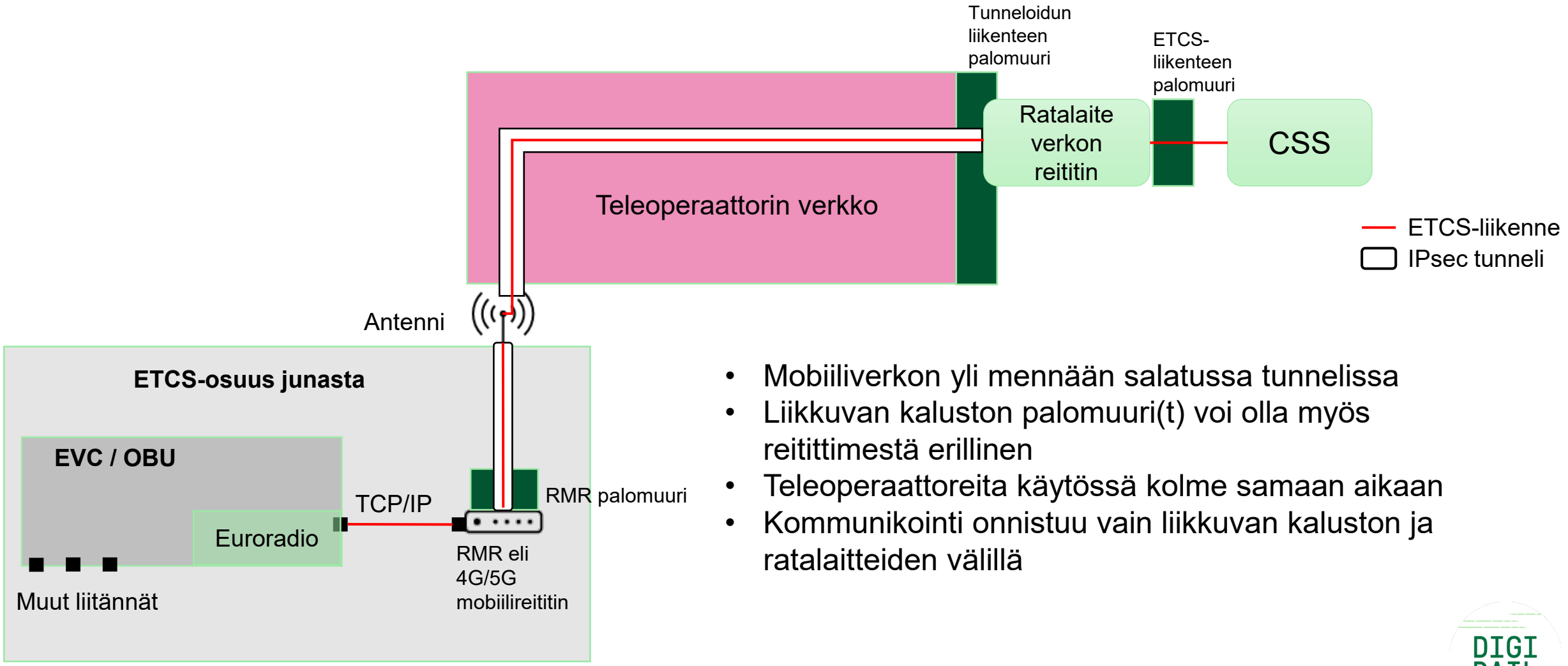
Kaluston omistajien näkökulma

- Mitä kalustonomistajat voivat tehdä uhkien torjumiseksi
  - Hallintajärjestelmä
  - Toimitusketjunhallinta
  - Vaatimukset hankinnoissa
- Yhteistyö eri osapuolten kanssa
  - Digiradan kybernyrkki
  - Raide YTR
  - …



DIGI RAIL

Yksinkertaistettu arkkitehtuuri



- Mobiiliverkon yli mennään salatussa tunnelissa
- Liikkuvan kaluston palomuuri(t) voi olla myös reitittimestä erillinen
- Teleoperaattoreita käytössä kolme samaan aikaan
- Kommunikointi onnistuu vain liikkuvan kaluston ja ratalaitteiden välillä

Uhat liikkuvan kaluston näkökulmasta

Funded by the European Union
NextGenerationEU

DIGI RAIL

Funded by
the European Union
NextGenerationEU

Palvelunestohyökkäykset

- Todennäköisin kohde kalustossa on monikanavareititin
- Laitteet ovat APN:n takana piilossa
    - Tarvitaan APN tiedot liikenteen reitittämiseen laitteelle
- Tietoliikenne kulkee vain yksityisiä verkkoja pitkin
- ETCS-yhteydelle on sallittu tietoliikenne vain kaluston ja CSS-verkon välillä

Verkon häirintä

- Kaikkia radioyhteyksiä voidaan häiritä elektromagneettisella säteilyllä
- Uudemmat verkkoteknologiat (4G/5G) kestävät häirintää paremmin
- Häirintää ei ole helppo toteuttaa laajalla alueella
- Käytössä on kolme yhteyttä, joten kaikkia pitäisi häiritä liikenteen estämiseksi

Funded by
the European Union
NextGenerationEU

Haittaohjelmat

- Asentamista varten tarvitaan tietoliikenneyhteys tai fyysinen pääsy kalustoon
- Kalustossa olevat reitittimet ovat eniten alttiita hyökkäyksille
- Tiedossa ei ole tapauksia, joissa ETCS-laitteisiin olisi asennettu haittaohjelmia

Toimitusketjuun liittyvät hyökkäykset

- Tärkeitä toimitusketjuja ovat tietoliikenneoperaattorit ja laitetoimittajat
- Suurimmat hyökkäyspinta-alat ovat reitittimissä ja palomuureissa sekä mobiiliverkossa
- Case Puola: kaluston valmistaja väitetysti jättänyt kalustoon ominaisuuksia, jotka estävät kaluston käytön, mikäli sitä huolletaan muilla kuin heidän sallimilla varikoilla

DIGI
RAIL

Kybernyrkki

Funded by
the European Union
NextGenerationEU

- Perustettu helmikuussa 2024
- Kybernyrkki käsittelee kokonaisarkkitehtuurin asioita liittyen Digirataan ja ERTMS/ETCS kyberturvallisuuteen
- Kaikki kaluston omistajat ja operaattorit tervetulleita
- Kokouksissa voi myös kysyä mietityttäviä asioita
- Tarjotaan apua kyberin kanssa työskentelyyn

DIGI
RAIL

Funded by
the European Union
NextGenerationEU

Cyber Security
Danish OBU Experience
2024-03-12

DIGI
RAIL

Funded by
the European Union
NextGenerationEU

Danish OBU Experience

Agenda

- The Danish Signalling Programme
- On-Board – Technical Overview
- The Authority Approval Process
- ERA / One Stop Shop
- Cyber Security Aspects

Martin Allesen

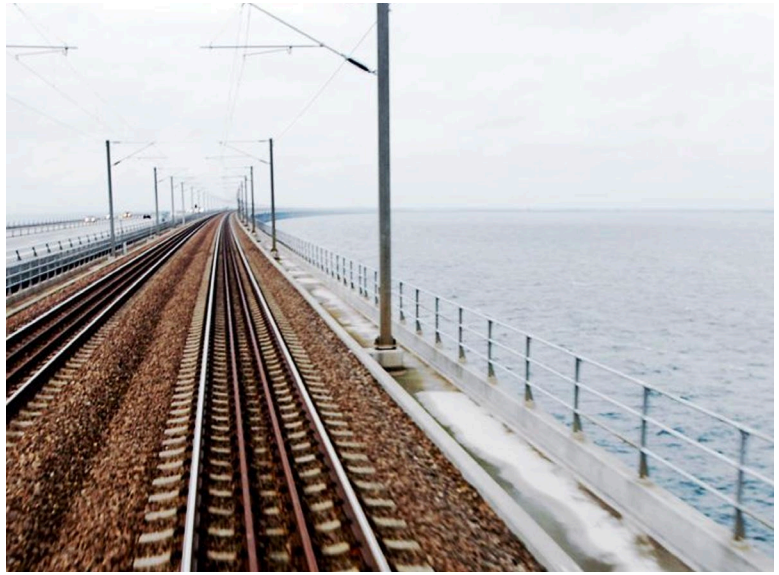
- Background
  - B.Sc.EE. - Digital Electronics / Computer Architecture / Communication Technology
  - Offshore – Electric Instrumentation
  - TÜV Certified Functional Safety Engineer
  - Rail Safety – CSM-RA, TSI
- Role in the Danish SP
  - Safety Advisor in Fjernbane On Board (FOB)
  - Change Management
  - Requirements Capture
  - DoV and Technical Files
  - ERADIS registration

The Danish Signalling Programme

- **Trackside**
  - Infrastructure Manager - BaneDanmark
  - Cover both operation and Infrastructure management
  - Establish ERTMS on East and West
  - New Operational rules for ERTMS

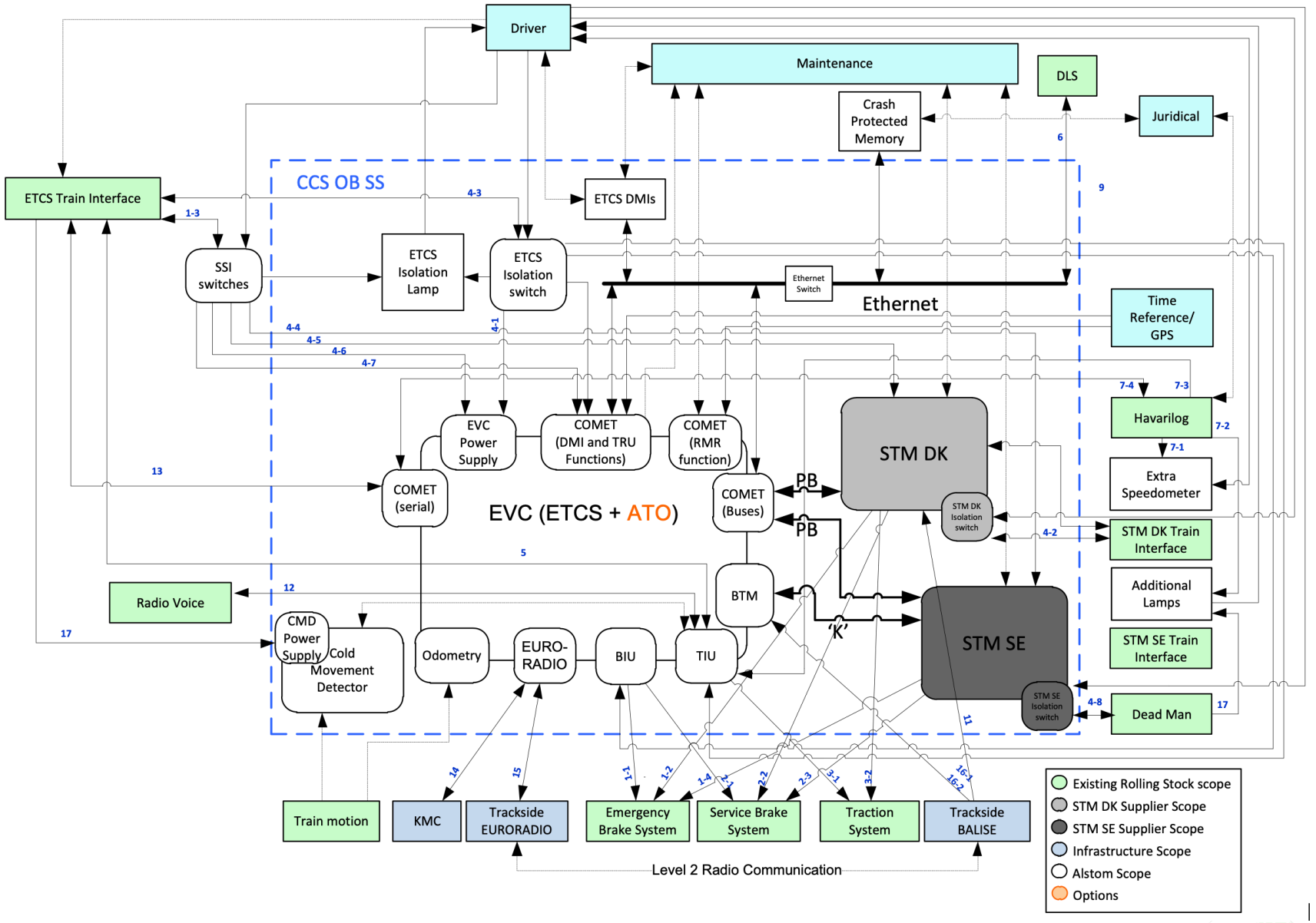
- **Rolling Stock - On-Board**
  - Political Decision -> part of Signalling Programme
  - Complete fitment by supplier (Alstom)
    - Design/installation/assessment
  - SP manage authorization process via ERA One Stop Shop
    - Many trains to operate in Sweden & Germany

  - **Railway undertaking:**
    - Main RU: Danish State Railways (DSB)
    - Smaller RU: Midjyske Jernbaner, Lokaltog, Arriva
    - Banedanmark Infra (yellow fleet),

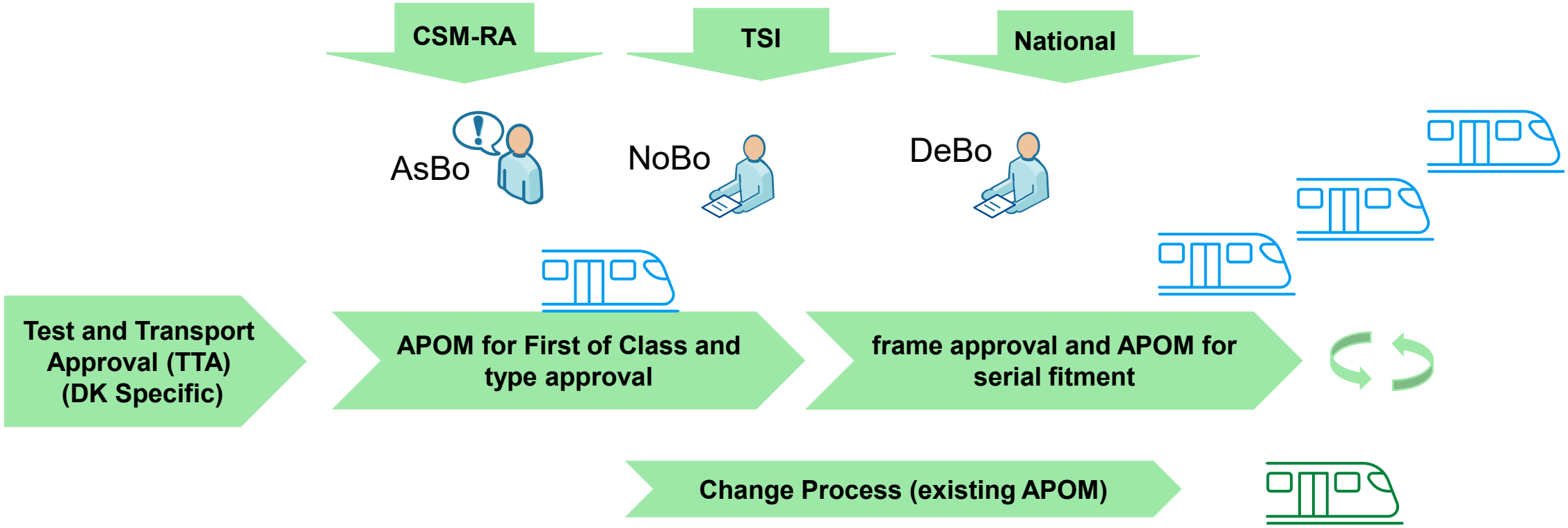


On-Board –
Technical Overview

- Hardware
  - On-Board
  - Fitment (Alstom)
  - Documentation (SP)
- Software
  - Alstom
  - Siemens (STM DK/SE)



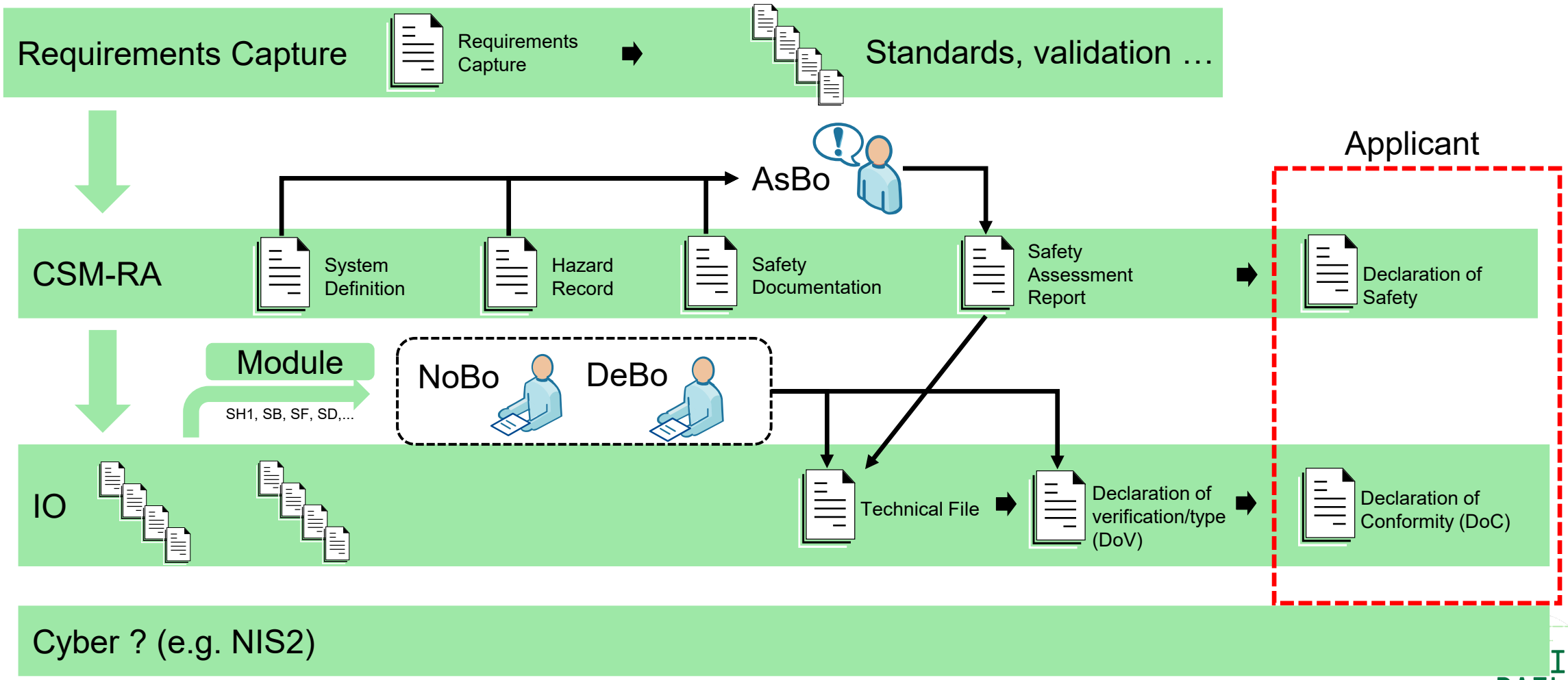
The Danish Authority Approval Process (EU)



- TSI – derogations
- 4th Railway package
- National legislation

- Supplier
- Strange problems : e.g. STM
- Cyber security

The Danish Authority Approval Process (EU)



SP Cyber security

- Security/vulnerability analysis in contract (2012)
- KMPG report on ERTMS security

- ETCS system is considered intrinsic secure
  - Confined system
  - Very complex -> require in-depth technical knowledge to attack

- Current Cyber security Focus:
  - ISO 27000 series business level compliance
  - OT not prioritized as ERTMS is viewed as intrinsic safe and there is no legal requirement

Summary

- The installation/approval process is complicated, time consuming and slow (roughly 18 months from design start to #1 installation)
- Requirements Capture is the basis for the approval process (Mapping of all legislative requirements to applicable standards and required validation and documentation).
- The foundation is ever-changing.
- Cyber Security is likely to become part of it.
- Consider this when deciding how to handle approval and fitment.
- ETCS is a confined, complicated and intrinsically secure system.

Funded by
the European Union
NextGenerationEU

DIGI RAIL

digirata.fi