Rail Baltica

Co-funded by
the European Union

Rail Baltica: Challenge Accepted!

The Integrator's Perspective

Mārtiņš Ķemme, IT Security Expert, RB Rail
Lille, France

2 October 2024

What is Rail Baltica?

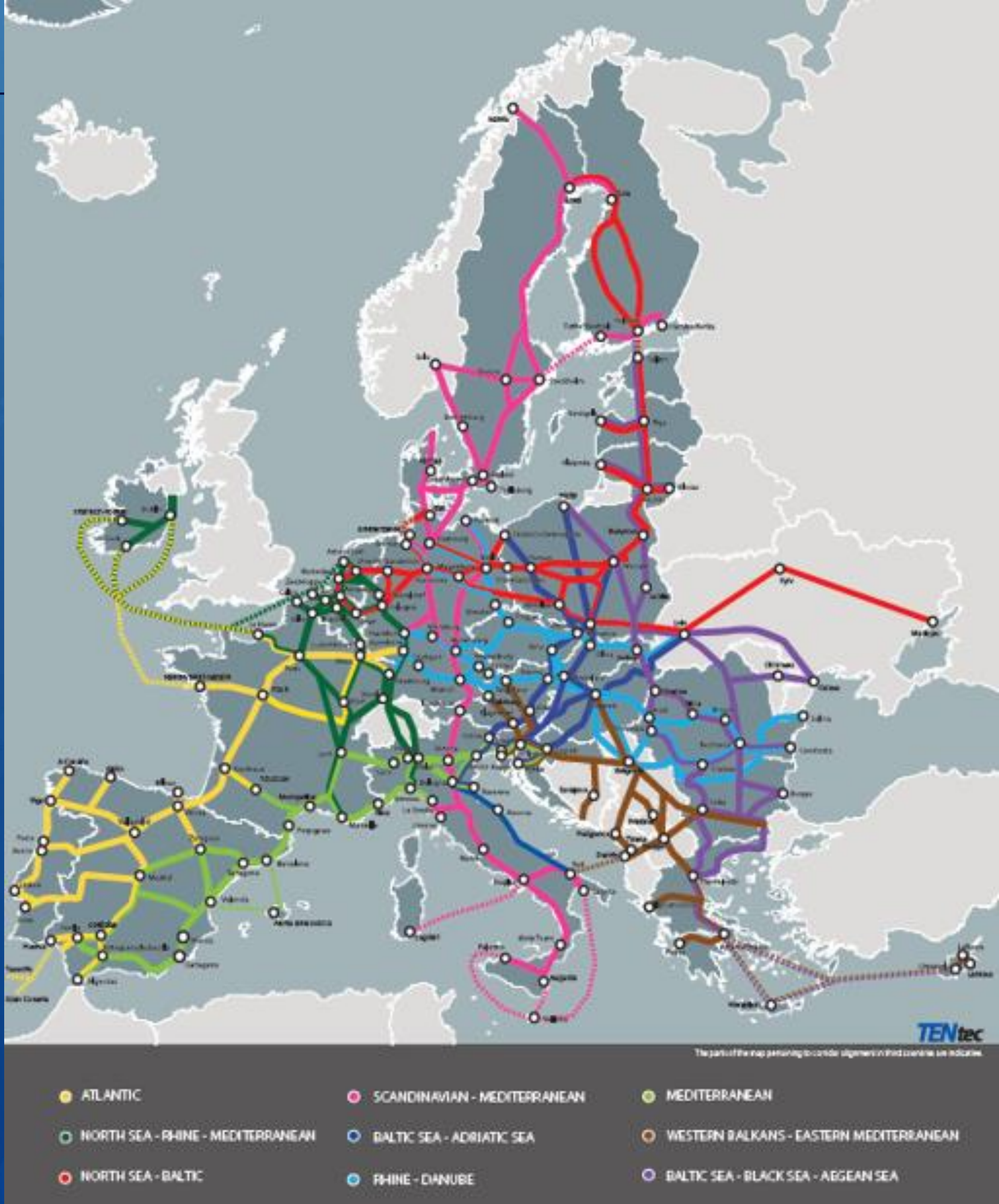
The Background

Rail Baltica

Co-funded by the European Union

Rail Baltica - not just a priority, but a geopolitical necessity

- Part of the North Sea-Baltic TEN-T Corridor
- Rail Baltica is included in the unified European transport corridor with Ukraine, as part of the Baltic Sea-Black Sea-Aegean Sea TEN-T corridor
- Bridging a missing transport link by 2030
- Delivering EU, regional, and national ambitions


TENtec
The parts of the map pertaining to corridor alignment in third countries are indicative.
ATLANTIC
SCANDINAVIAN - MEDITERRANEAN
MEDITERRANEAN
NORTH SEA - RHINE - MEDITERRANEAN
BALTIC SEA - ADRIATIC SEA
WESTERN BALKANS - EASTERN MEDITERRANEAN
NORTH SEA - BALTIC
RHINE - DANUBE
BALTIC SEA - BLACK SEA - AEGEAN SEA

Rail Baltica scope to ensure a functioning transport, military and economic corridor

7 international passenger stations
45 local passenger stations/stops

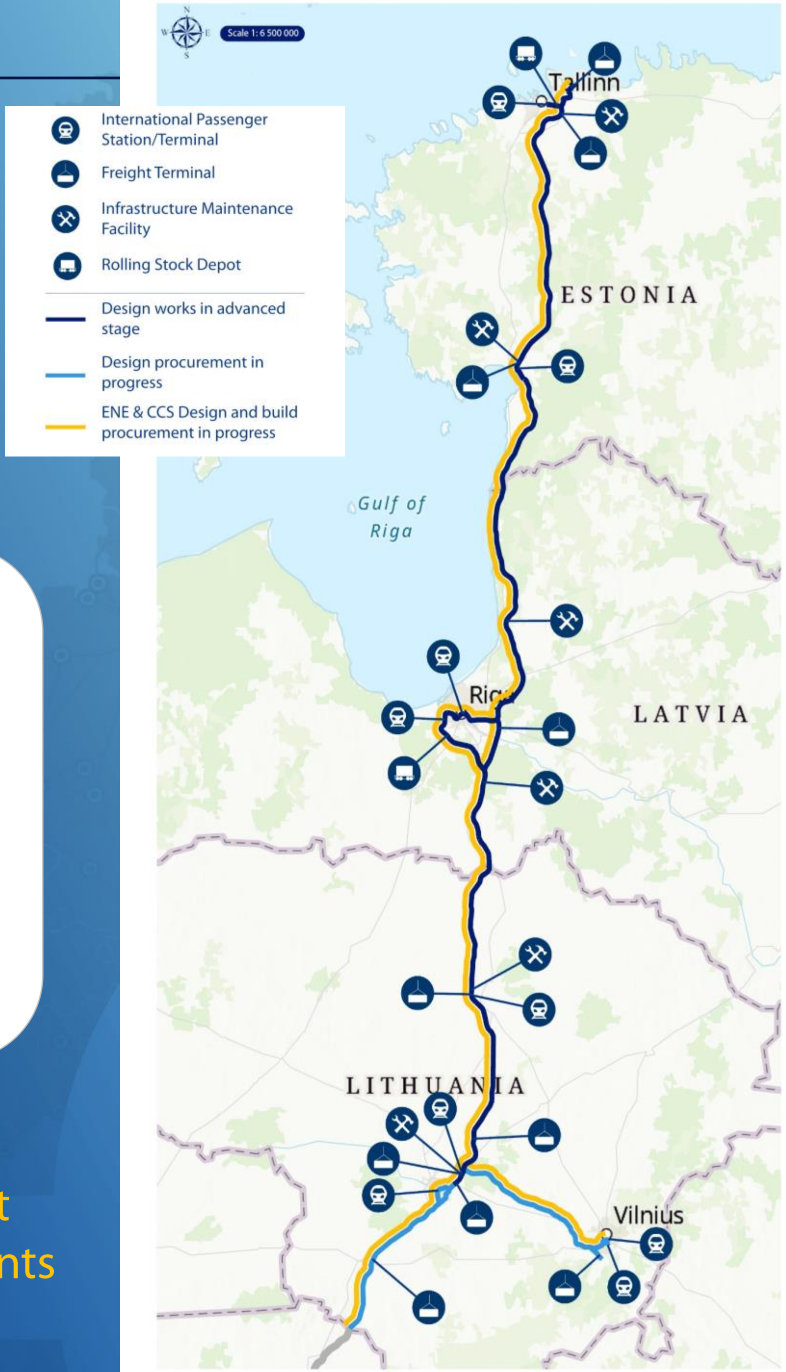
3 tunnels

> 90 structures (bridges, overpasses, viaducts, tunnels)

6 Infrastructure maintenance facilities

> 90 wildlife crossings (ecoducts, culverts, overpasses)

14 freight terminal + port connection


Scale 1: 6 500 000
International Passenger Station/Terminal
Freight Terminal
Infrastructure Maintenance Facility
Rolling Stock Depot
Design works in advanced stage
Design procurement in progress
ENE & CCS Design and build procurement in progress
Tallinn
ESTONIA
Gulf of Riga
Riga
LATVIA
LITHUANIA
Vilnius

International passenger transport I Cross-border regional passenger transport
Regional passenger transport I Freight transport I Military mobility requirements

15% of the mainline under construction in 2024

- Master designs for priority sections nearing completion
- Over 150 km of mainline under construction
- Consolidated material procurements in final stage
- Electrification and signaling subsystem (870 km) design and build procurement ongoing

Mainline embankment under construction contracts:
>300 km

Mainline embankment under ongoing tenders:
>200 km

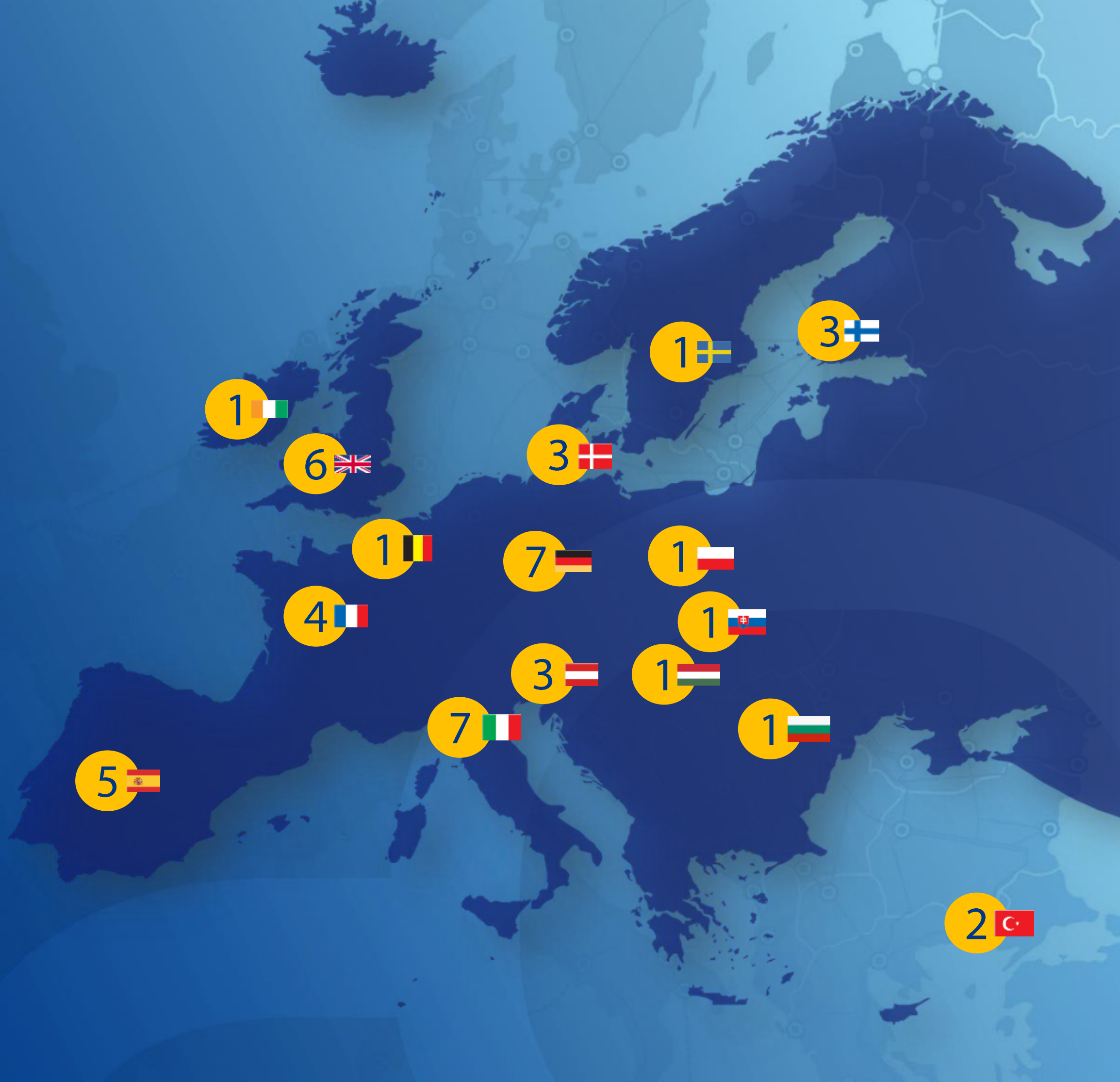
Rail Baltica

Co-funded by
the European Union

Over 300 international and Baltic-based suppliers

> 4.7bn EUR of suppliers' contracts signed

Austria	GrECo · SWIETELSKY · TU Graz
Belgium	BESIX
Bulgaria	EKI
Denmark	PLH · COWI · RAMBØLL
Finland	YIT · AIG · GRK
France	egis · CERTIFER · SNCF · SYSTRA · EIFFAGE
Germany	ermcon · railistics · PTV VISSIM · OBERMEYER · DB · TÜV · Gauff ETC Solutions
Hungary	BCG
Ireland	Bentley
Italy	Sintagma · ITALFERR GRUPPO FERROVIE DELLO STATO · IDS INGEGNERIA DEI SISTEMI · 3TI PROGETTI · RIZZANI DE ECCHER
Poland	VINTAGE CONSULTING · budimex
Slovakia	Valbek Prodex
Spain	ineco · prointec · IDOM · renfe · Ardanuy
Sweden	SWECO
Turkey	YÜKSEL PROJE · prm
U.K.	Network Certification Body · Hogan Lovells · LINUM CONSULT · ATKINS · AECOM · ZAHA HADID ARCHITECTS



Partnerships and potential suppliers' interest from the US, Japan, and other non-EU countries

How to make Rail Baltica cybersecure?

The Approach

opportunities

challenges

GREENFIELD

adoption of latest technologies for CCS (like FRMCS)
and for cybersecurity;
joint initiatives with existing 1520mm network

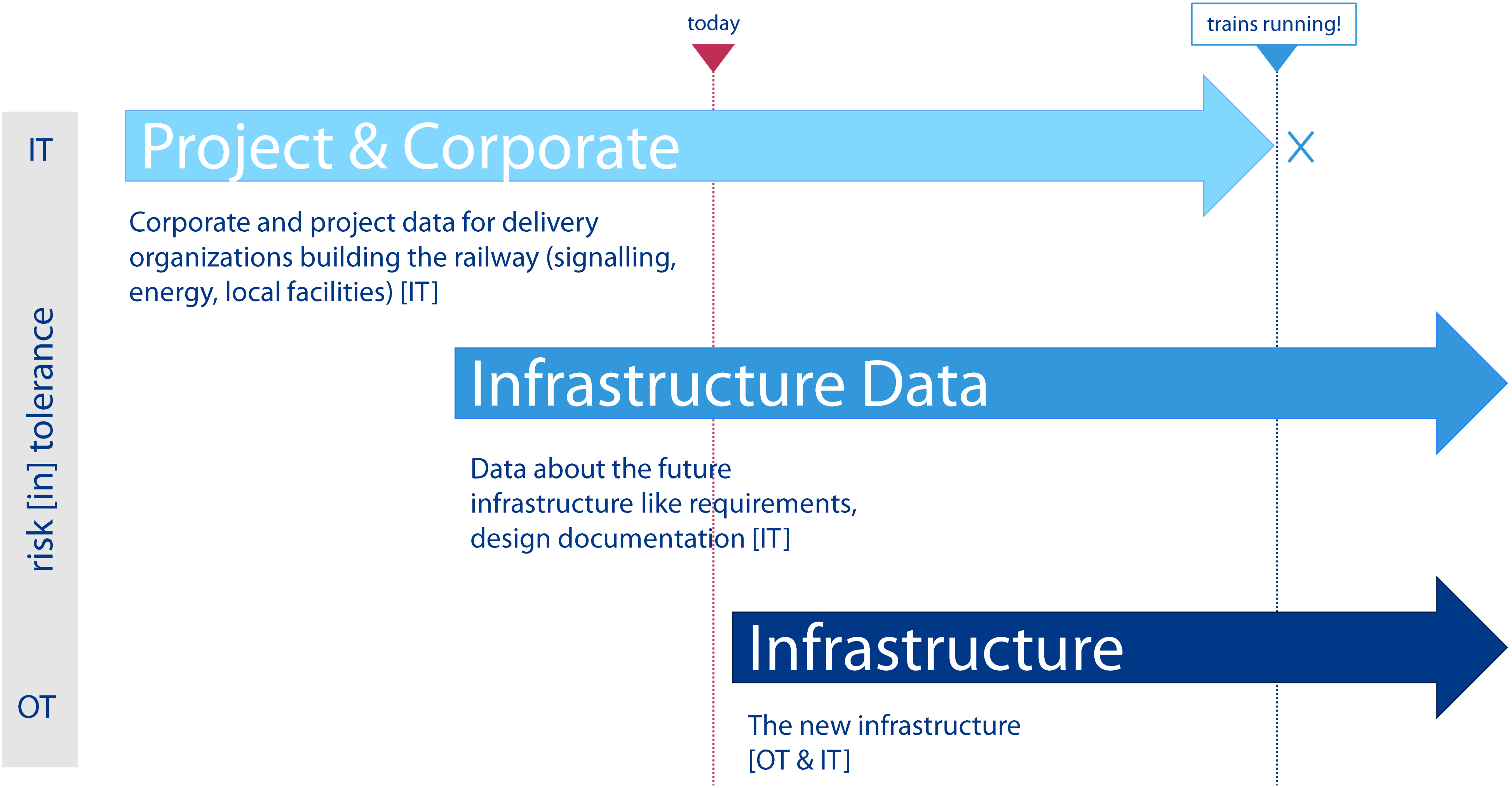
3

countries
legislative basis
ministries
beneficiaries

JOINT EFFORTS vs COUNTRY SEPARATION,

e.g., for Cybersecurity Operation Centre, supply chain management

Cybersecurity Scope



today

trains running!

IT

risk [in] tolerance

OT

Project & Corporate

Corporate and project data for delivery organizations building the railway (signalling, energy, local facilities) [IT]

Infrastructure Data

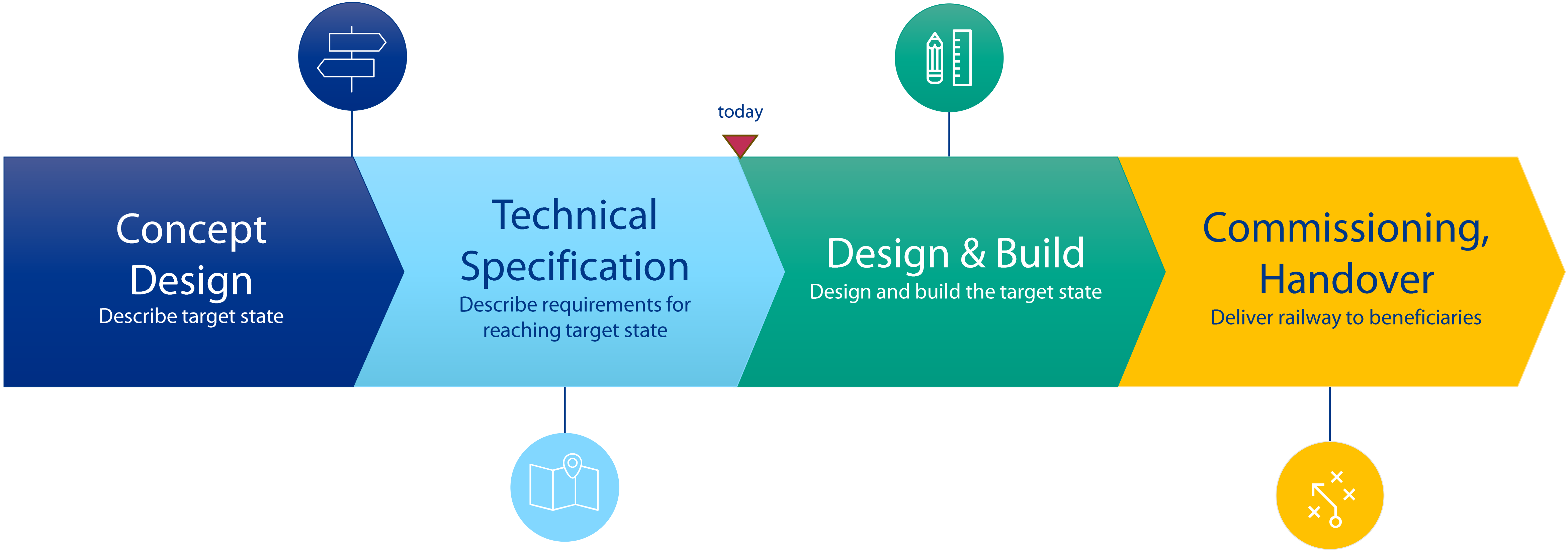
Data about the future infrastructure like requirements, design documentation [IT]

Infrastructure

The new infrastructure [OT & IT]

Transitioning from description of the target state to requirements was not easy – it required different approach to cybersecurity requirements (security solutions → security principles)

Cybersecurity management, incl. risk assessment, requirement elaboration, supply chain management, assurance



today
Concept Design
Describe target state
Technical Specification
Describe requirements for reaching target state
Design & Build
Design and build the target state
Commissioning, Handover
Deliver railway to beneficiaries

Threat identification. TS defines core cybersecurity requirements (principles) and is basis for procurement of design and build

Cyber-secure operation and maintenance of the to-be-infrastructure. Transfer of assets and processes

NIS2 as one of requirement drivers

It is critical infrastructure even before it is ready

01 Risk Management

- Applies to the entire scope
- Run Cyber-SOC forthe project
- Design Cyber-SOC for operations
- Plan and design data centre security
- Design for crypto-agility
- Collaboration between countries

02 Incident Management and Reporting

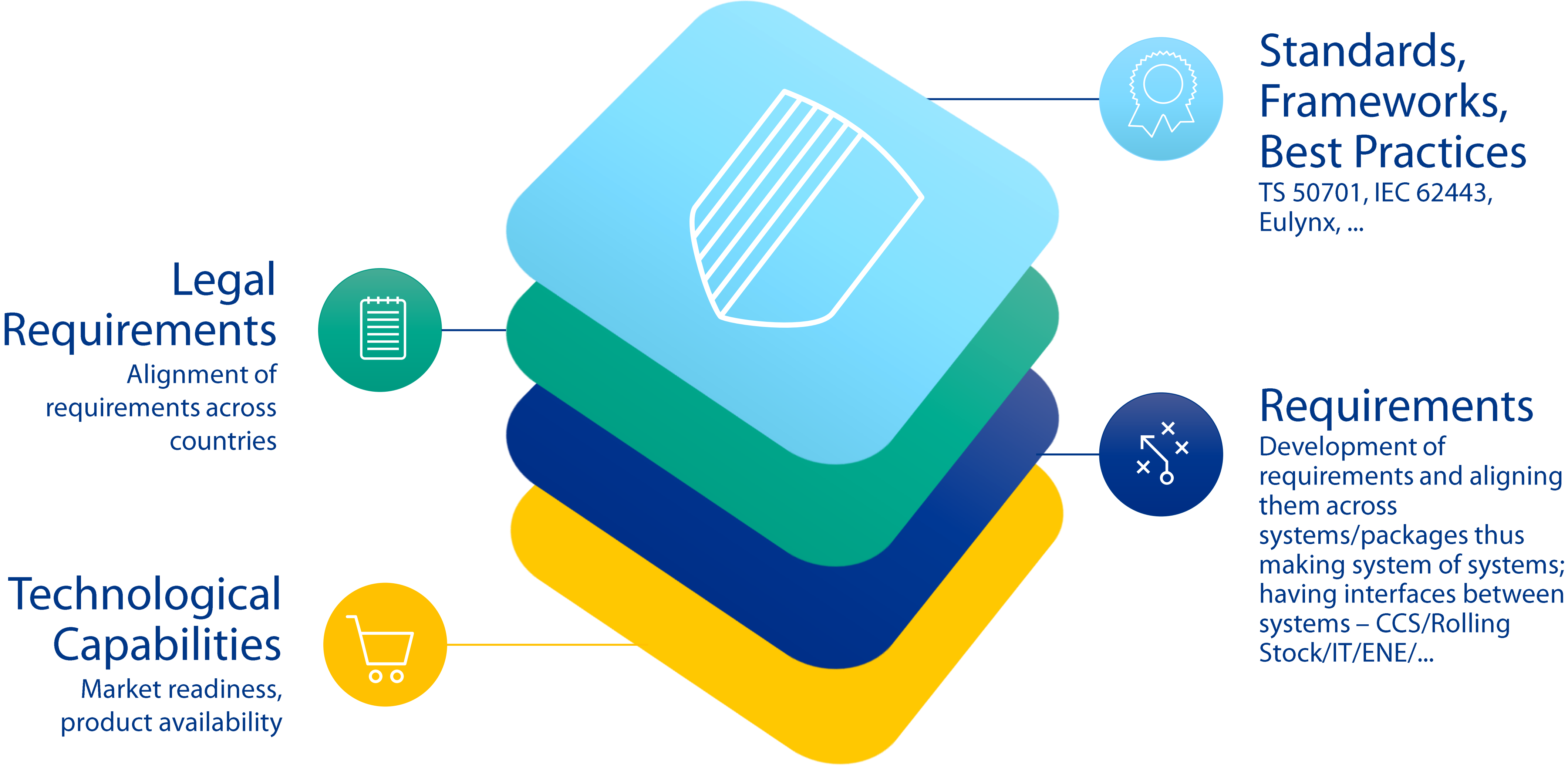
- Handling corporate IT incidents
- Handling IT & OT incidents during design and build phases
- Laying the foundation for incident handling during operations
- Cooperation with national CSIRTs

03 Supply Chain Management

- Procurement requirements
- SCM during design and build

04 Awareness and Education

- Project and corporate environment



Standards, Frameworks, Best Practices

TS 50701, IEC 62443, Eulynx, ...

Legal Requirements

Alignment of requirements across countries

Requirements

Development of requirements and aligning them across systems/packages thus making system of systems; having interfaces between systems – CCS/Rolling Stock/IT/ENE/...

Technological Capabilities

Market readiness, product availability

NIS2 | Eulynx

A good match

SOC
Security Operations Centre

CSIRT
Incident Response Team

SIEM
Security Incident & Event Management

PKI
Public Key Infrastructure

IAM
Identity and Access Management

SIC
Security Incident Centre

ISAC
Information Sharing and Analysis

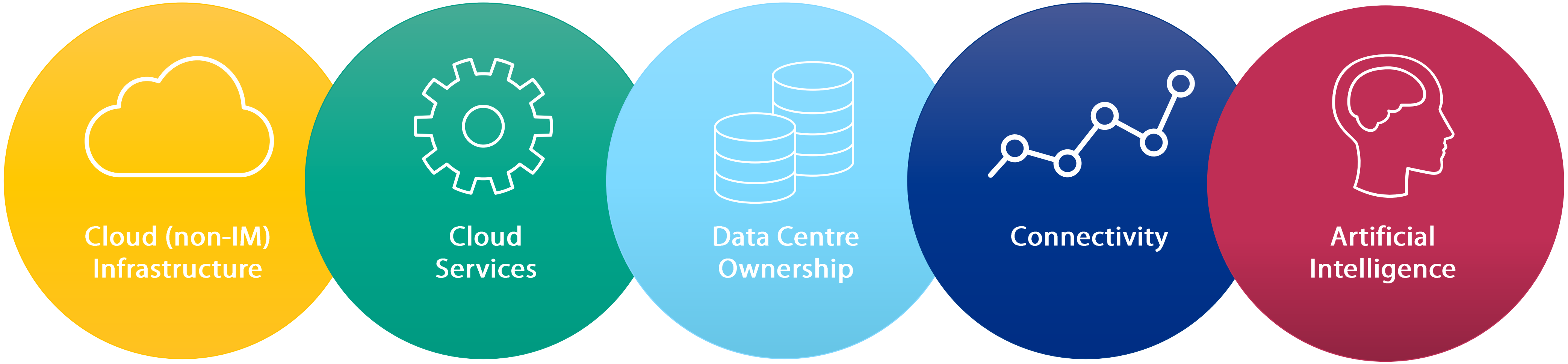
CLOCK
Time Sync

BACKUP
Backup & Recovery

Logging
Logging Services

Challenges, Tolerances, Risk Appetite

Looking for the red lines. Differs across packages.



Cloud (non-IM) Infrastructure

To be or not to be?

Cloud Services

These are part of this anyway, right?

Data Centre Ownership

Infra Manager owned / State owned / other

Connectivity

Who owns the cable? Who manages the network? Who can see the data?

Artificial Intelligence

Runs trains? No! Fights against threats? Absolutely!

All-in-all NIS2 directive is helpful in setting common policy and requirements for data centres, cloud services, AI, etc.

Key Takeaways

The Importance and Value of the Cybersecurity

Cybersecurity is not a domain on its own or in isolation; it is part of all aspects and activities of the project. Digital components and services are ubiquitous; therefore cybersecurity must be there. As railways become more digital, new spectrum of threats arises.

Cybersecurity considerations are impacting architecture of the system(s).

NIS2 is helpful although national legal acts are still fresh.

It is our responsibility to make a safe environment and provide feedback rather than passively wait for NIS2 v2.

Thank you!

martins.kemme@railbaltica.org