



4th ERA-ENISA Conference on Cybersecurity in Railways

***"Importance of cybersecurity strategies from
Europe's Rail SRG perspective"***

02 OCTOBER 2024 – Lille, France





Role of the Europe's Rail States Representatives Group in Cyber security



Agencies, associations	and partnerships
	 European Space Agency
	 European Union Agency for the Space Programme
	 JOINT UNDERTAKING

ER ISAC MEMBERS

Members



Partners



NIS2 and its impacts

11 sectors of high criticality:

- transport,
- energy,
- digital infrastructure
- ICT services management,
- space

-
- banking,
 - financial market infrastructure,
 - healthcare,
 - drinking water,
 - wastewater,
 - public administration.

In member states it is going to be necessary to ensure that regulated services (high criticality) in transport and related fields are fully interoperable.

Railway system belongs to the critical – but most probably to the

SUPER CRITICAL infrastructure



Is there a need for a new cyber security TSI then?

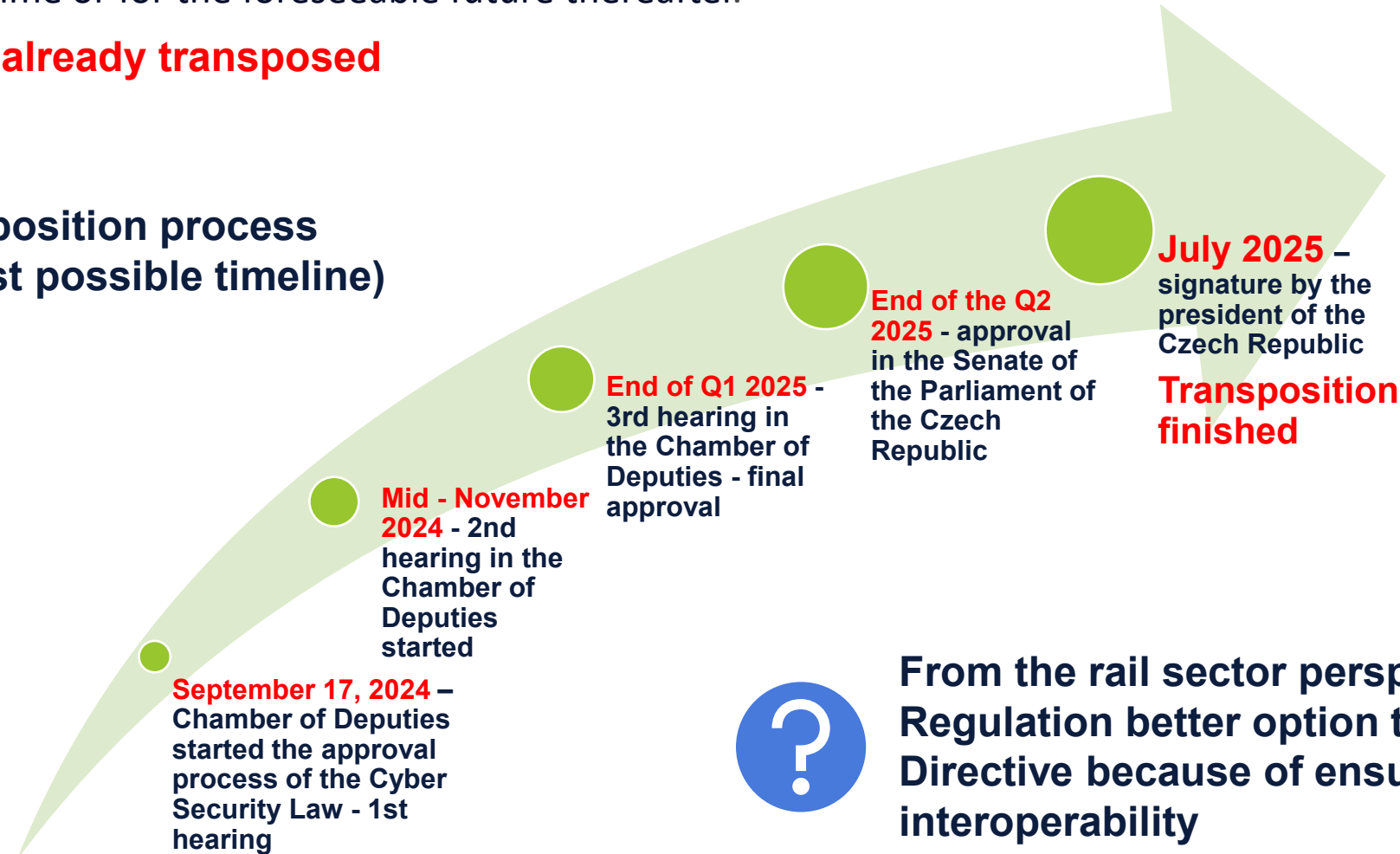
NIS2 – transposition process in the Czech Republic

As of October 17, 2024, the EU's mandatory for transposition of the cybersecurity directive NIS 2 will be implemented and is expected to enter into force at that time or for the foreseeable future thereafter.

HR, IT, BE - already transposed



Transposition process (fastest possible timeline)



From the rail sector perspective is Regulation better option than Directive because of ensuring interoperability

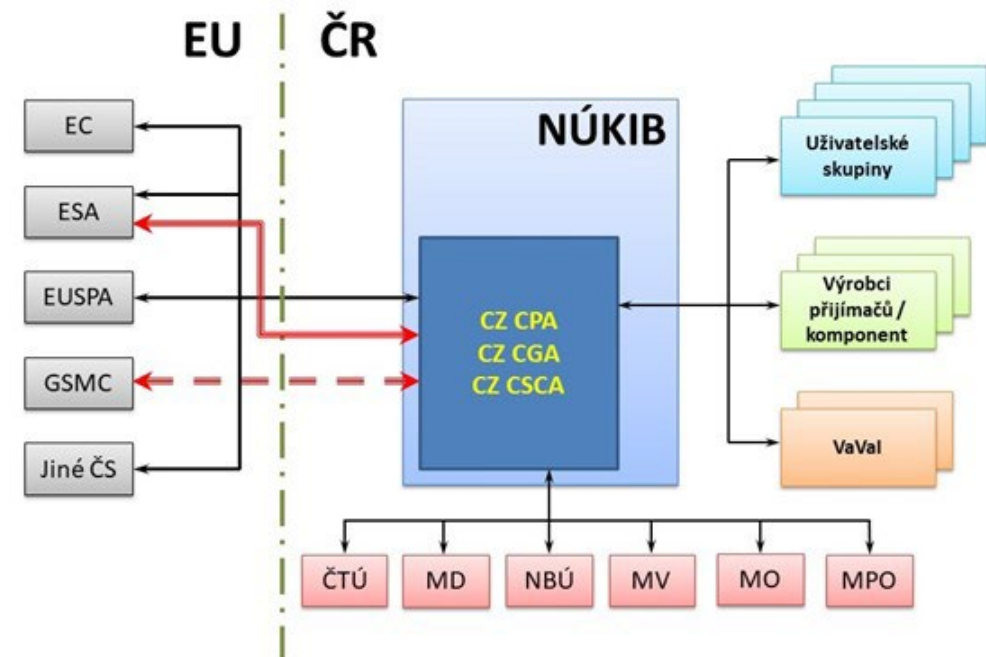
Space and NIS2 impact

This is very specific area with a specific regulatory rules.

EU Space Programme

The EU Space Programme is the first integrated space programme created by the European Union to support space-related policies. It addresses societal challenges, technological innovation, supporting the EU's internal market, but also ensuring protection against and prevention of various security threats. The programme consists of several components. The security aspects of the individual components of the EU Space Programme in the Czech Republic are managed by the NACIB. The Ministry of Transport is the manager of the entire EU Space Programme in the Czech Republic. Components of the EU Space Programme:

- Galileo
- EGNOS
- USC
- GOVSATCOM
- Copernicus



NIS2 transposition – MS example

Vládní návrh
ZÁKON
ze dne 2024
o kybernetické bezpečnosti

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ KYBERNETICKÁ BEZPEČNOST

Hlava I Základní ustanovení

§ 1 Předmět úpravy

(1) Tento zákon upravuje práva a povinnosti osob, organizačních složek státu a dalších orgánů veřejné moci v oblasti zajišťování kybernetické bezpečnosti a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) a dalších orgánů veřejné moci.

(2) Tento zákon se vztahuje na osoby, které jsou usazeny na území České republiky. Tento zákon se dále vztahuje na osoby, které na území České republiky zajišťují síť nebo poskytují služby elektronických komunikací podle jiného právního předpisu¹⁾, bez ohledu na místo jejich usazení.

(3) Tento zákon zapracovává příslušný předpis Evropské unie²⁾ a zároveň navazuje na přímo použitelné předpisy Evropské unie³⁾.

¹⁾ Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

²⁾ Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

³⁾ Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU.

Rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejně regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo.

Hlava II
Poskytovatel regulované služby
Díl 1
Regulovaná služba a režim jejího poskytovatele

§ 3 Regulated service

A regulated service is a service which was deemed as such by the Agency as per § 6 par.

2.

Podmínky pro registraci regulované služby

§ 4

(1) Podmínky pro registraci regulated services are splněny v případě, že

a) it is a service of significance for the security of important social or economic activities, or for the security in the Czech Republic in some of these fields:

1. veřejná správa a výkon veřejné moci.
2. energy.
3. výrobní průmysl.
4. potravinářský průmysl.
5. chemický průmysl.
6. vodní hospodářství.
7. odpadové hospodářství.
8. transport.
9. digital infrastructure and services.
10. finanční trh.
11. zdravotnictví.
12. science, research and education.
13. poštovní a kurýrní služby.
14. defence industry.
15. space industry a

b) poskytovatel služby je středním nebo velkým podnikem ve smyslu doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (dále jen „doporučení Komise 2003/361/ES“)⁶⁾, nebo je významný

⁶⁾ Sdělení Ministerstva průmyslu a obchodu č. 7/2023 o vyhlášení českého znění doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

NIS2 transposition – MS example

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB 

Reporting of cybernetic security incidents



Incident is a breach of security of information within assets.
Information security is ensuring confidentiality, integrity, and availability of information and data.



The law is expected to come to force on 1st January 2025.

Providers of regulated services start reporting cybernetic security incidents **within 1 year at the latest** after the delivery of the decision on registration.

WHAT TO REPORT AND TO WHOM?



Higher level obliged persons

All incidents, that

- are of cybernetic origin, **and**
- intent cannot be ruled out.

Incidents are reported to **NÚKIB**.

Lower level obliged persons

All incidents, that

- are of cybernetic origin,
- have significant impact (as defined in legislation) **and**
- intent cannot be ruled out.

Incidents are reported to **CERT**.

NIS2 and its general impacts

Cyber security

is one of the most important parts of all processes in the entire railway system – starting from

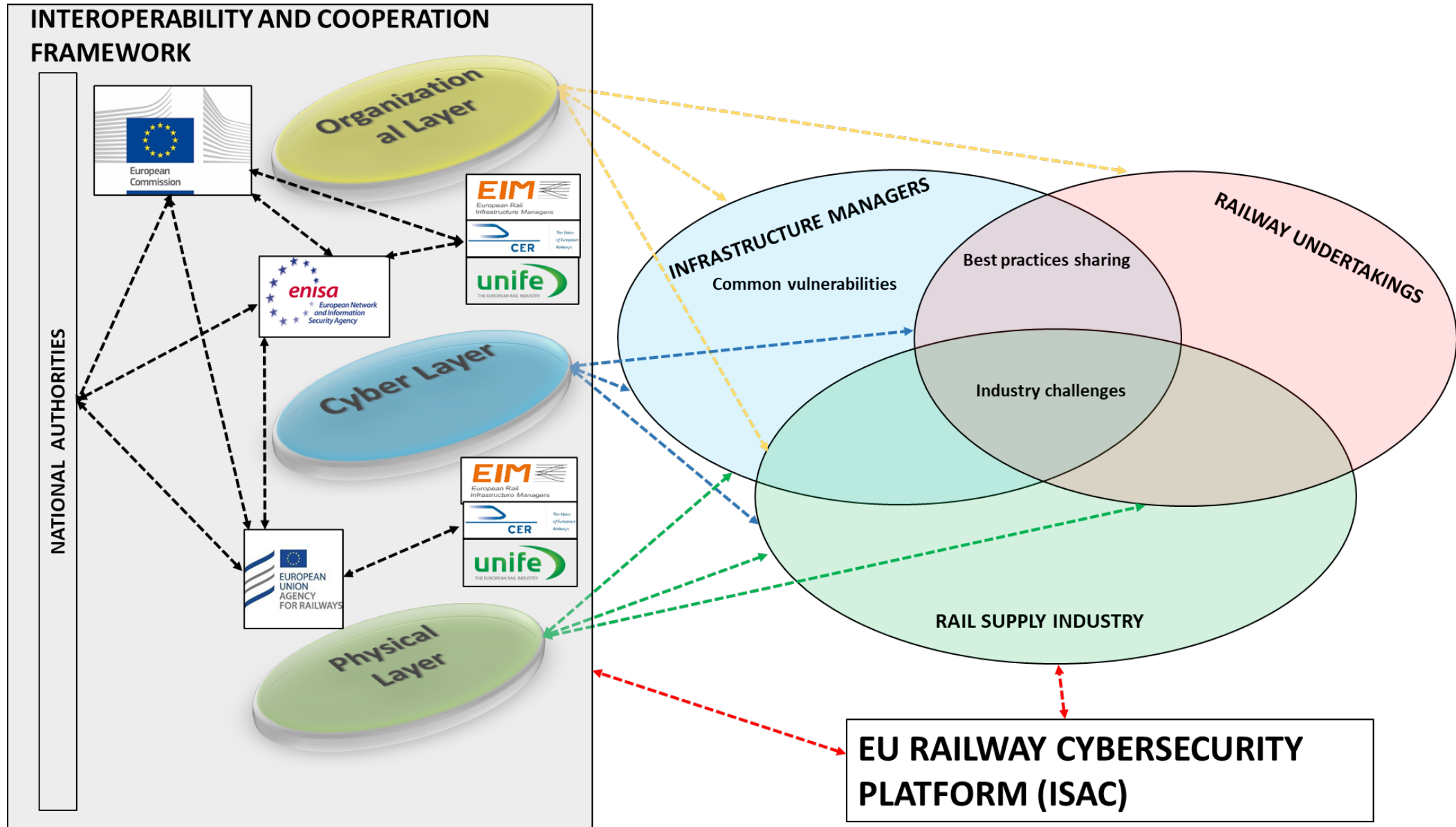
- production of rolling stock,
- signalling systems, and all infrastructure subsystems and components
- monitoring and control systems,
- transport planning

to

- provisioning processes to the sale of travel documents to passengers
- provision of consignment notes and other necessary documents for the transport of goods.

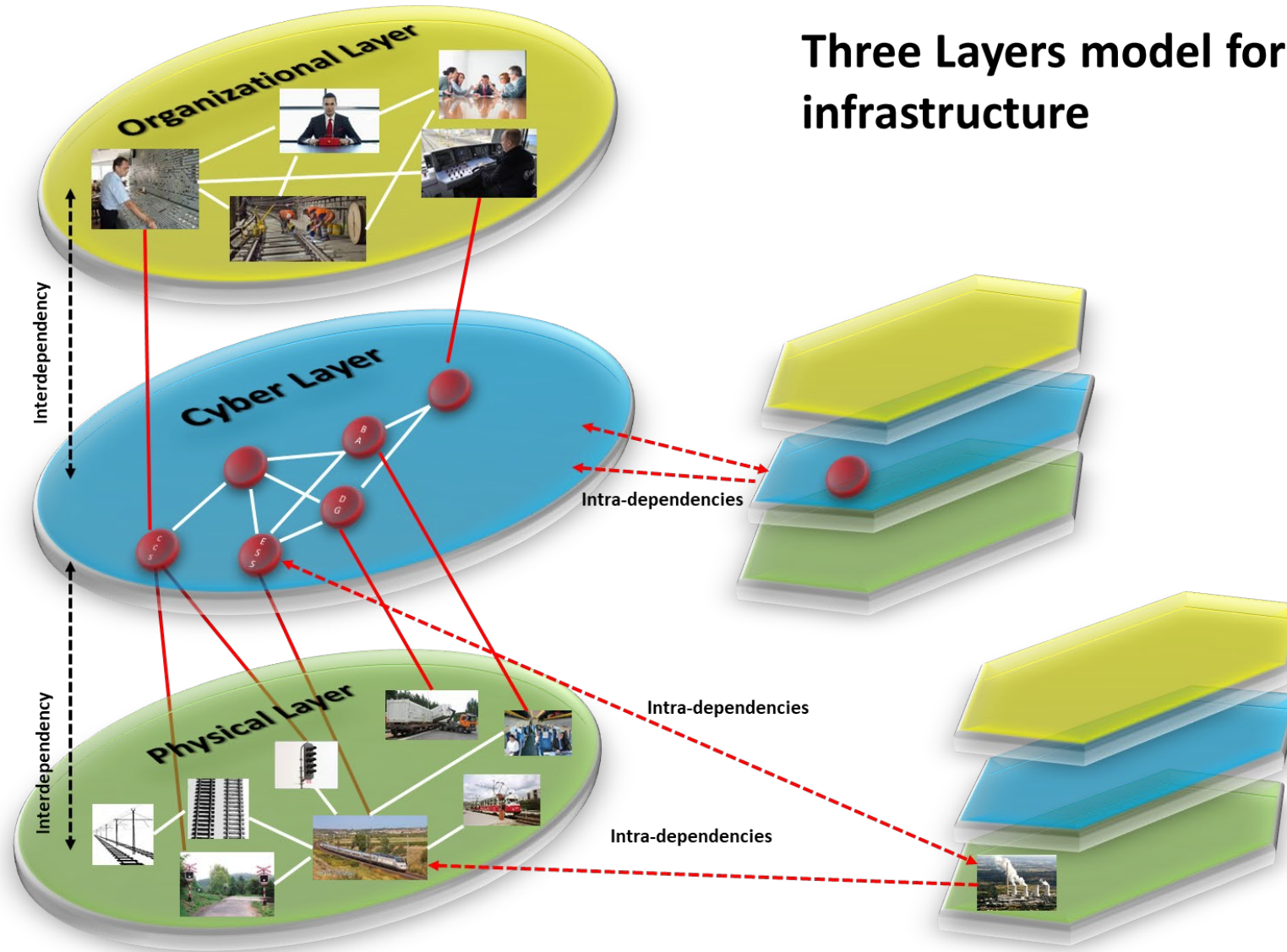
	
<p>Technical Specifications for Interoperability (TSI)</p> 	  
	
<p>Regulation (EU) 2020/1056</p>   <p>CIV – tickets RID - safety list CIM – consignment note</p>	<p>Project </p>   <p>OTIF Intergovernmental Organisation for International Carriage by Rail RID 2023 Regulations concerning the International Carriage of Dangerous Goods by Rail</p>

NIS2 and interoperability

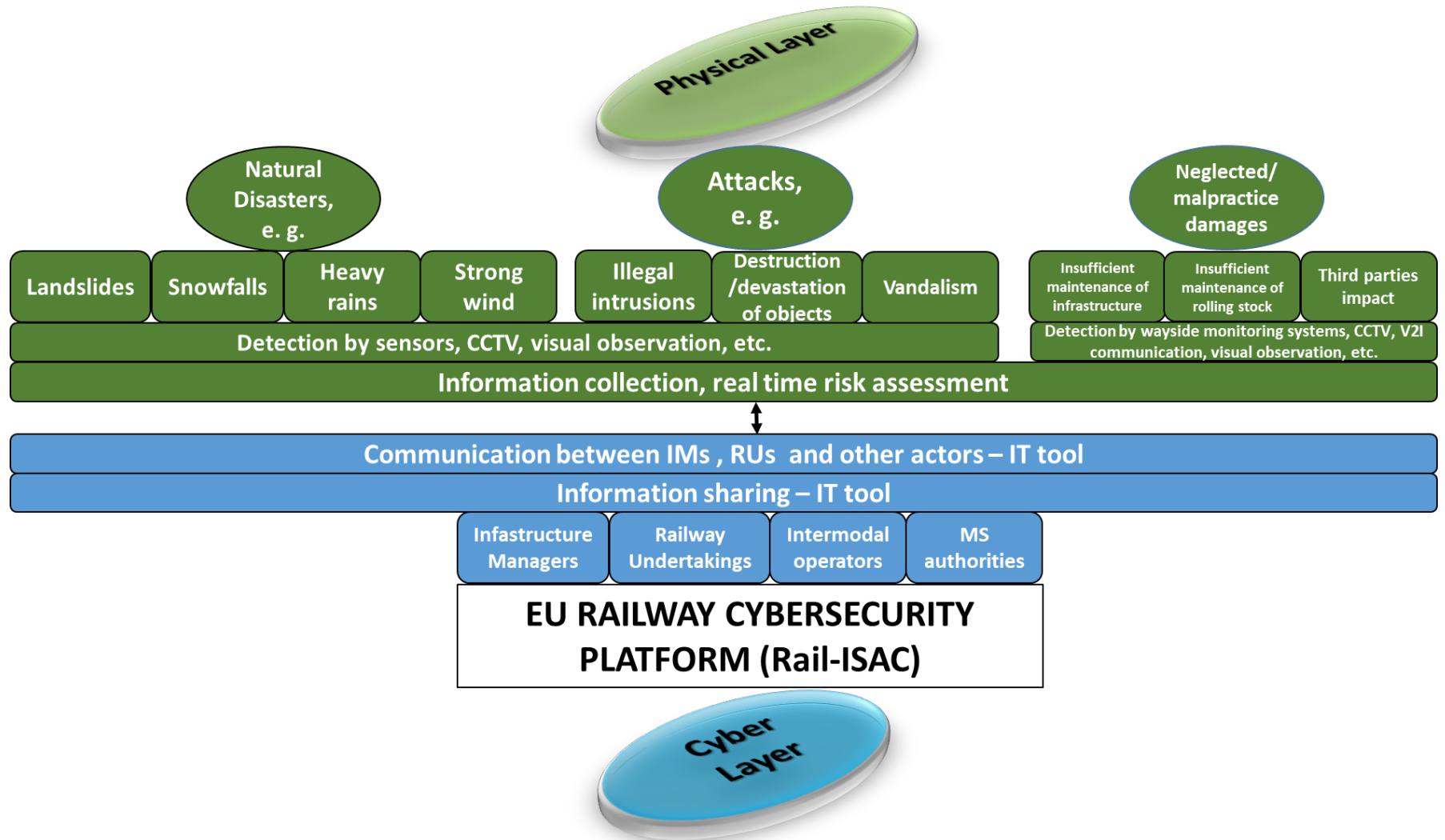


NIS2 and its impact to rail operation

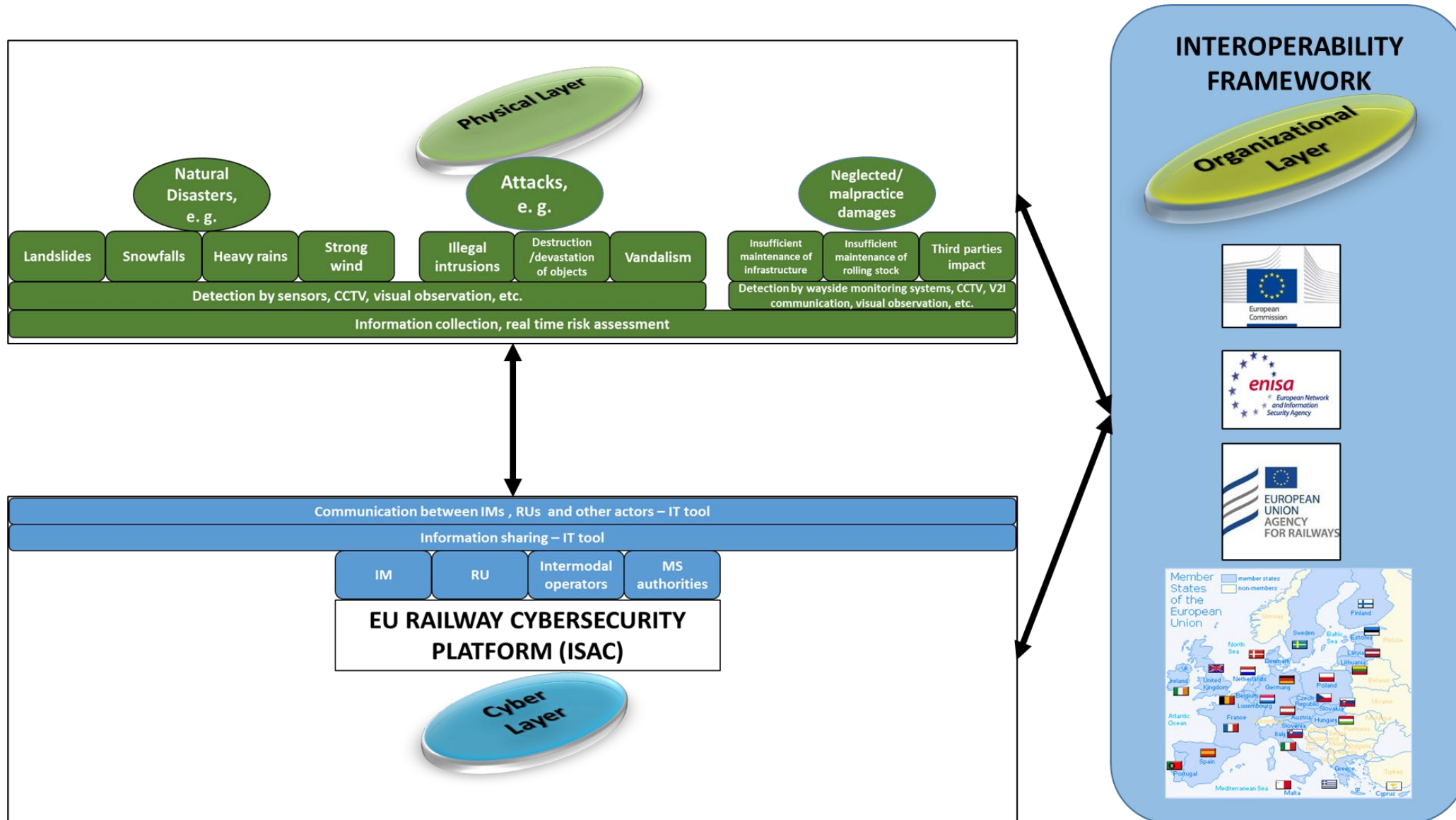
Three Layers model for critical infrastructure



Impact of space technologies used in digitalization and automation of the rail system to cyber security

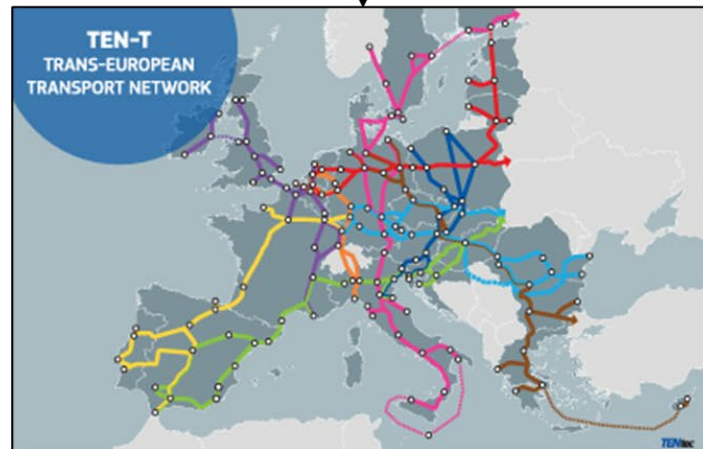


Interoperability framework in each field of the rail system (incl. telematics as non-safety related TSI)

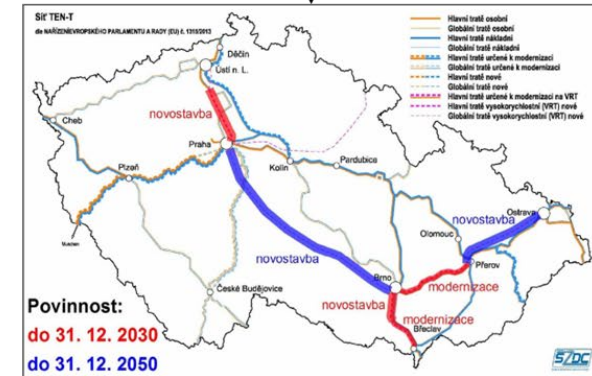
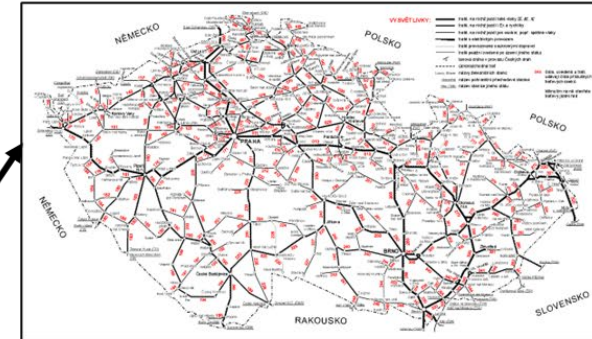


Reference to specific rail freight transport (military and RID)

EU LEVEL



Member State LEVEL



Key safety and operational indicators

From the point of view of the Member States, rail transport is a key strategic sector which must ensure the operation of other key sectors at all circumstances.


These sectors are

- **defence,**
- **national internal security,**
- **integrated rescue system and**
- **strategic industries.**

Considering these strategic needs of the Member States and the EU as a whole, it is therefore necessary to consider how to ensure that the **development of new smart information technologies, artificial intelligence, and automation** of transport processes is not the **main risk factor or a limiting factor in safety** of the rail system.

It is therefore also necessary to consider that critical safety on-board and ground systems should be implemented in a way that **allows for them to be circumvented** in the case of a cyber threat and, importantly, **redundancy** needs to be ensured in **"crisis mode"** with a minimal IT support.

Europe's Rail SRG Members

EU 		EU 		EU 	
AT		FI		LV	
BE		FR		MT	
BG		GR		NL	
CY		HR		PL	
CZ		HU		PT	
DE		IE		RO	
DK		IT		SE	
EE		LT		SI	
ES		LU		SK	
Non-EU		Non-EU		Non-EU	
AL		NO		UK	
IL		TR		Transport Community (Western Balkan)	

4th ERA-ENISA Conference on Cybersecurity in Railways

Europe's Rail Founding Members

