Cybersecurity conference

The link between Safety Culture & Cyber-security

02-03/10/2024| Lille

EUROPEAN UNION AGENCY FOR RAILWAYS

Photo: Adobe Stock / by_Tarasylo

EUROPEAN UNION AGENCY FOR RAILWAYS

Content

- Railway Safety Culture
- Cyberthreat in railway
- The link between safety culture and cybersecurity in railways

Railway Safety Culture

EUROPEAN UNION AGENCY FOR RAILWAYS

- Safety Culture Model
- Safety Climate Survey
- Organisational Just Culture
- Safety Culture Declaration
- Safety Leadership
- Safety Culture Oversight

EUROPEAN UNION AGENCY FOR RAILWAYS

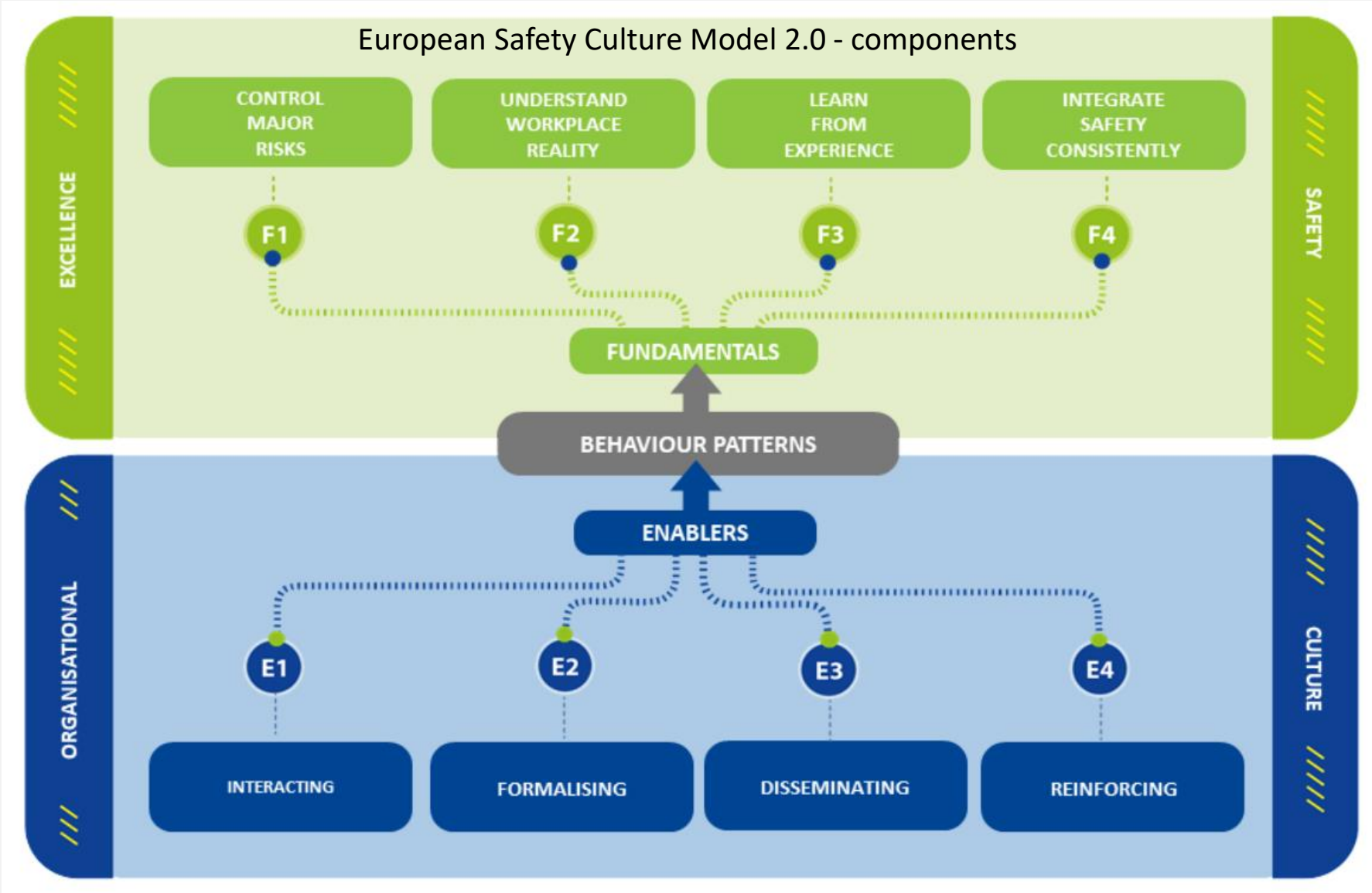
Safety Culture Model

Model building blocks:

•**Cultural Enablers**: levers through which an organisational culture develops;

•**Behaviour Patterns**: shared ways of thinking and acting which convey the organisational culture;

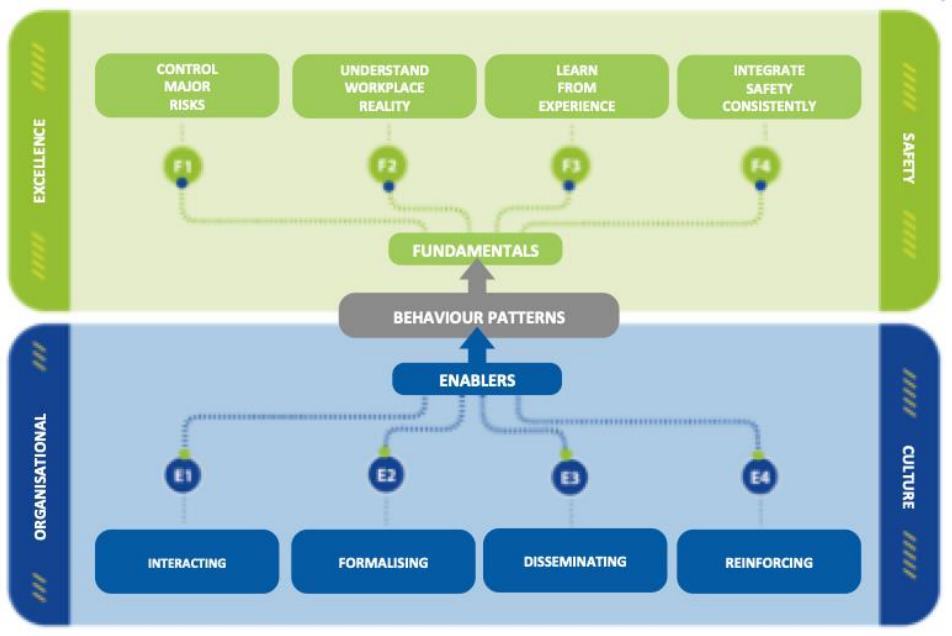
•**Railway Safety Fundamentals**: core principles which must be reflected by behaviour patterns to achieve sustainable safety performance and organisational excellence.



EUROPEAN UNION AGENCY FOR RAILWAYS

Safety Culture Programme

To devise *dissemination* and *evaluation instruments* to support the development of a positive safety culture within the Single European Railway Area



Key principle: any deliverable is tested with partner organisations

Programme Management, Knowledge and Strategy

EUROCONTROL

ICSI Institut pour une culture de sécurité industrielle

WANO GLOBAL LEADERSHIP IN NUCLEAR SAFETY

EUROPEAN UNION AGENCY FOR RAILWAYS

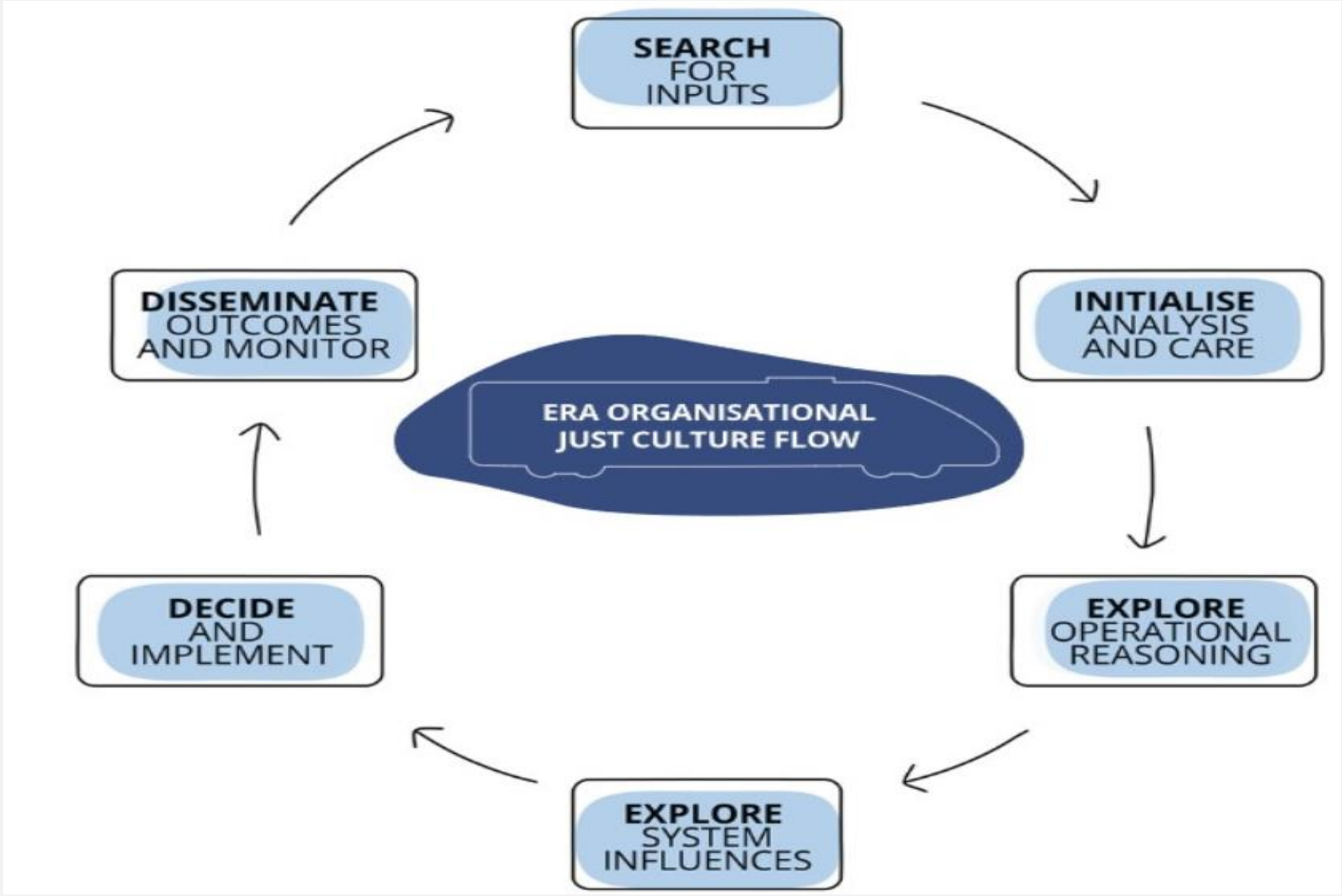
Organisational Just Culture

Developing an OJC

- dedication and consistency
- open and respectful dialogue
  (staff report safety issues)
- analyse and act upon
  to improve

to achieve an..
appropriate, sustainable, safe operational performance

Free online basic module:
ERA Organisational Just Culture flow



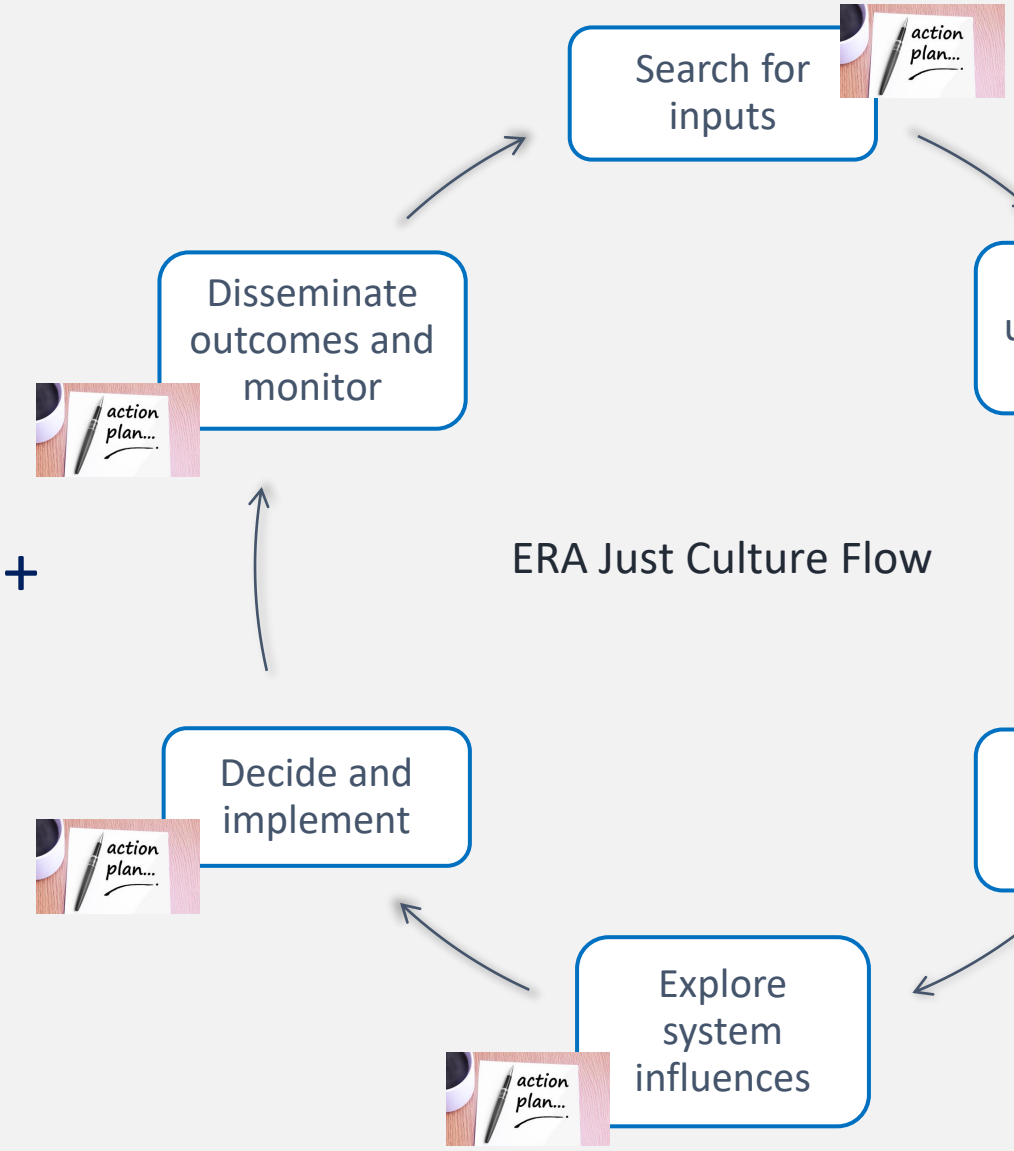
EUROPEAN UNION AGENCY FOR RAILWAYS

ERA Just Culture Flow

Global Overview and Action Plan

Basics of Just Culture

+



+

Integrating Just Culture

EUROPEAN UNION AGENCY FOR RAILWAYS

Safety management system

What is the SMS **for** ?

Who is **responsible** for safe railway operation ?

Safety Management System (SMS)

the organisation, arrangements and procedures
established by an IM or a RU
to ensure the safe management
of its operations

RU.s IM.s are responsible for the SMS,
each one for its own part of the system
and its safe operation

https://www.era.europa.eu/can-we-help-you/faq/300_en

EUROPEAN UNION AGENCY FOR RAILWAYS

RU – IM interface risks

RU.s IM.s shall co-operate together to manage the **interface risks**.

Through their SMS, RU.s IM.s demonstrate that they have the ability to identify, assess, control risks which arise from its own activities and **risks caused by others***.

National safety authority has still the ability **to check** effectively the **co-operation arrangements** put in place by RU.s IM.s during its supervision activities.

EUROPEAN UNION AGENCY FOR RAILWAYS

Risk based approach

RU.s IM.s **continuous control** of (identified) risks and co-operate with each other for shared interface risks.

New/amended rules shall be **traced back** to the original identified risk.

Difficult to **relate** numerous old **rules to risks**. There is no single solution.

Discuss possible solutions (e.g. grouping of rules, cross-references) and their implementation together with the **safety certification body**.

EUROPEAN UNION AGENCY FOR RAILWAYS

Significant change in safety & RA

Regulation (EU) No 402/2013 criteria for **assessing the significance** of a safety-related change, adequate documentation to justify the decision.

The question on the significance of a safety-related change does not release the railway company from its **obligation to perform a proper risk assessment**

to demonstrate that the level of safety is maintained or even improved

when the change is significant, in addition to the RA, an **independent assessment body** must be appointed,
to verify independently the correct application of the RA - Annex I Reg.402-2013

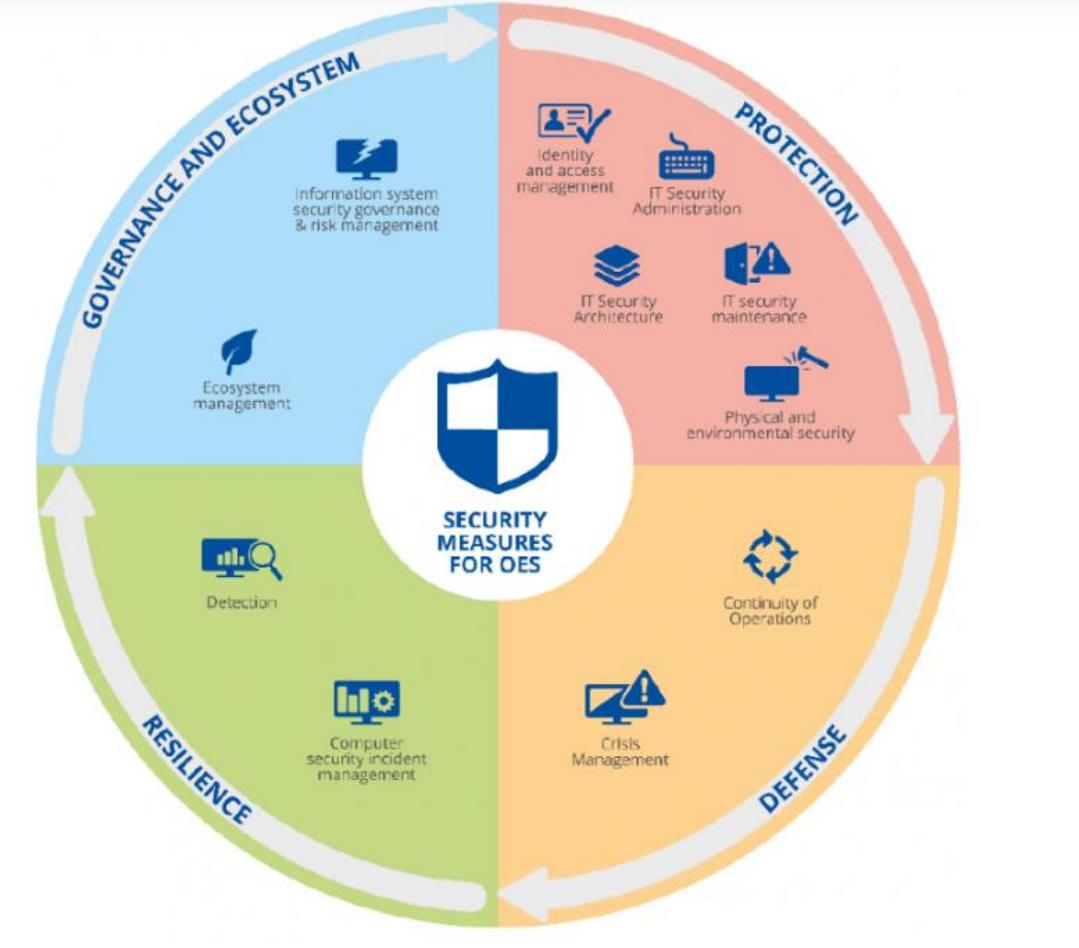
Cyber-threats in railways

EUROPEAN
UNION
AGENCY
FOR RAILWAYS

Photo: Adobe Stock / by_Tarasylo

EUROPEAN UNION AGENCY FOR RAILWAYS

Cyberthreat in railway



"Cyber" **risks cannot be dissociated** from railway risks

Boundary between railway safety and cybersecurity to be determined…
Essential to clarify the functioning at the **interface** between the "worlds" SMS - IMS.

The **increasing degree of connectivity** of the infrastructure and rolling stock (i.e. DAC – FDFTO) is creating a significant increase of their attack surface

Programmable devices exposed to cyberthreats when "**not connected**", besides communication, we need to protect design, production, maintenance (standards, certifications, …)

Security measures for railway operators defined as operators of essential services (OES)

EUROPEAN UNION AGENCY FOR RAILWAYS

Cyberthreat in railway

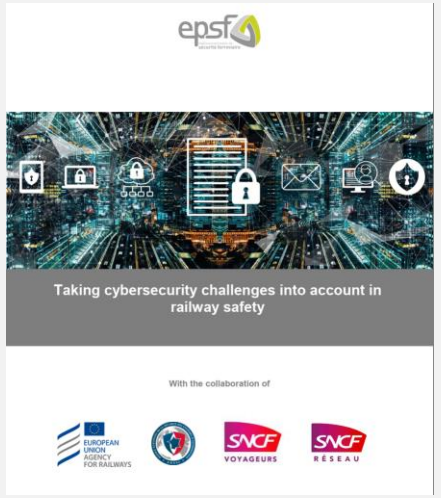
What to highlight:

- the respective scopes of the railway and of the cybersecurity **regulatory frameworks**;

- the ongoing works aiming to **build a shared framework** between **safety and cybersecurity**, and to strengthen the way the cybersecurity dimension is taken into account in the railway sector and in the other means of transport;

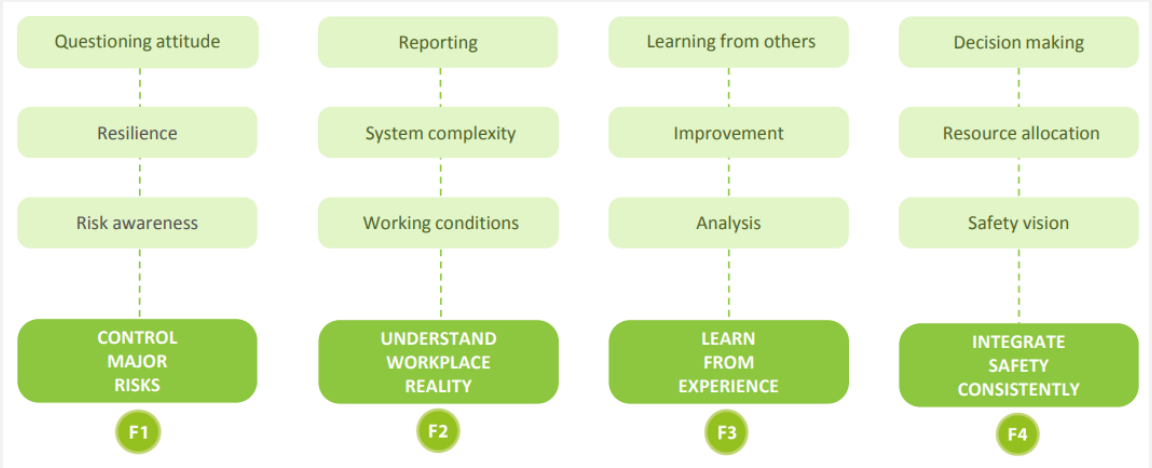
- the operational subjects that have already been identified and that justify the need for a clear **operating framework** in the area of **"overall" safety**;

- **recommendations** stemming from the discussions and exchanges



Taking cybersecurity challenges into account in railway safety

Railway Safety Fundamentals: Keywords



EUROPEAN UNION AGENCY FOR RAILWAYS

Regulatory frameworks

Terms & competences are different:

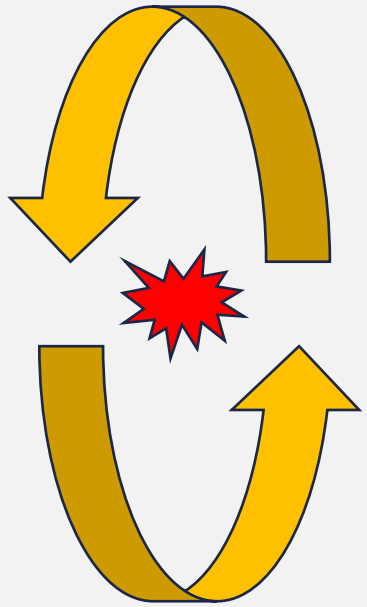
Railway safety - overall functioning of the system, subsystems (INF, RST, CCS, OPE, ...).
The risks are above all, technical and environmental.

Operating safety - ability of the components (brakes, etc.) of a sub-system to meet one or more functions

(safety of technical sub-systems)

Cybersecurity - technologies, processes, practices to protect the networks, computers, data against
attacks, damage and unauthorised access.

IT “security” includes cybersecurity & physical safety.



IEC 62443 – Series of standards that define requirements and processes for implementing and maintaining **electronically secure industrial automation** and control systems (IACS).

CLC/TS 50701 - Technical Specification introducing requirements and recommendations to **address cyber security** within the **railway** sector.

IEC 63452 standard: aims to create a strong, clear, and implementable framework which will **enhance the security of rail systems** across rolling stock, fixed installations, management systems and additional services.

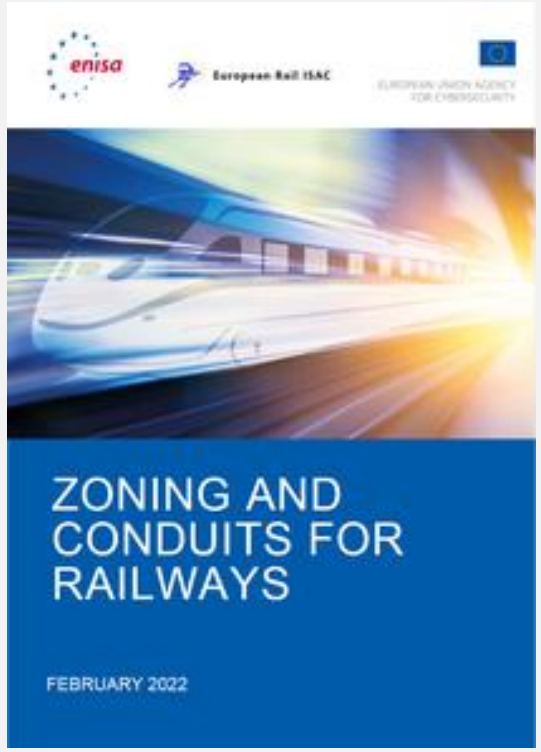
EUROPEAN UNION AGENCY FOR RAILWAYS

Implement and share

Building cyber secure Railway Infrastructure 2022

ENISA & European Rail Information Sharing and Analysis Center (ISAC) report

sectorial implementation of the NIS Directive.



ENISA Transport Threat Landscape

mapping and studying cyber incidents 2021-2022

identifies prime threats, actors and trends

(aviation, maritime, railway, road)

The link between safety culture and cybersecurity, in railways

EUROPEAN UNION AGENCY FOR RAILWAYS

Photo: Adobe Stock / by_Tarasylo

EUROPEAN UNION AGENCY FOR RAILWAYS

Risk Management Perspective

Risk Management Perspective:

Both cybersecurity and safety culture focus on identifying and mitigating risks. A strong safety culture encourages proactive identification and management of safety risks within an organisation.

Similarly, cybersecurity involves identifying vulnerabilities and threats to digital assets and infrastructure and implementing measures to mitigate these risks.

Integrating cybersecurity into safety culture frameworks ensures that risks to both physical safety and digital security are addressed comprehensively.

Examples of link to the Safety Culture Model

F1.1 - Risk awareness
F1.3 – Questioning attitude

EUROPEAN UNION AGENCY FOR RAILWAYS

Organisational Awareness and Training

Organisational Awareness and Training

A robust safety culture emphasizes the importance of continuous awareness and training for employees at all levels. This includes understanding safety protocols, reporting procedures, and maintaining vigilance to potential hazards.

Similarly, in the context of cybersecurity, awareness and training programs are essential to educate railway personnel about cyber threats, phishing attacks, secure handling of data, and the use of digital systems safely.

By integrating\linking cybersecurity training into existing safety culture initiatives, railway organisations can create a more holistic approach to risk management.

Examples of link to the Safety Culture Model
E2.3 Organisational systems

E3.2 Competence management
F2.2 System complexity

EUROPEAN UNION AGENCY FOR RAILWAYS

Resilience and Incident Response

Building A Resilient Organisational Culture

for Crisis Preparedness

(image: FasterCapital)

Resilience and Incident Response

A strong safety culture fosters resilience by ensuring that the personnel is prepared to respond effectively to incidents and emergencies.

This readiness includes clear communication channels, rapid response protocols, and post-incident analysis to prevent future occurrences.

In the realm of cybersecurity, resilience involves having robust incident response plans, including procedures for detecting, containing, and recovering from cyber incidents.

By aligning incident response strategies across safety and cybersecurity domains, railway organisations can enhance their overall operational resilience.

Examples of link to the Safety Culture Model *F1.2 Resilience* *F2.3 Reporting*
F3.2 Analysis (for incident response) *F3.3 Learning from others (cross-sector mitigation)*

EUROPEAN UNION AGENCY FOR RAILWAYS

Regulatory Compliance

Regulatory Compliance
Both safety and cybersecurity in railways are subject to regulatory frameworks and standards.

When apply for a safety certificate, it is required to railway operators to demonstrate adherence to safety management systems (SMS) and cybersecurity standards to ensure operational safety and data protection (area of potential conflict, transparency vs privacy).

Integrating cybersecurity measures into safety culture frameworks helps ensure compliance with regulatory requirements and demonstrates a commitment to maintaining high standards of safety and security.

Examples of link to the Safety Culture Model *E2.1 Roles, responsibilities* *E2.2 Organisational design* *E2.3 Organisational systems* *E1.3 Regulatory relationships*

EUROPEAN UNION AGENCY FOR RAILWAYS

Cultural Norms, Organisational Values

Cultural Norms and Organisational Values:

Safety culture extends beyond formal procedures and regulations to encompass organisational norms, attitudes (leadership), and values regarding safety.

Similarly, promoting a cybersecurity-aware culture involves embedding security consciousness into everyday practices and decision-making processes across all levels of the organisation.

By fostering a culture where safety and cybersecurity are seen as shared responsibilities, railway organisations can cultivate an environment where both physical and digital aspects of operational integrity are prioritised.

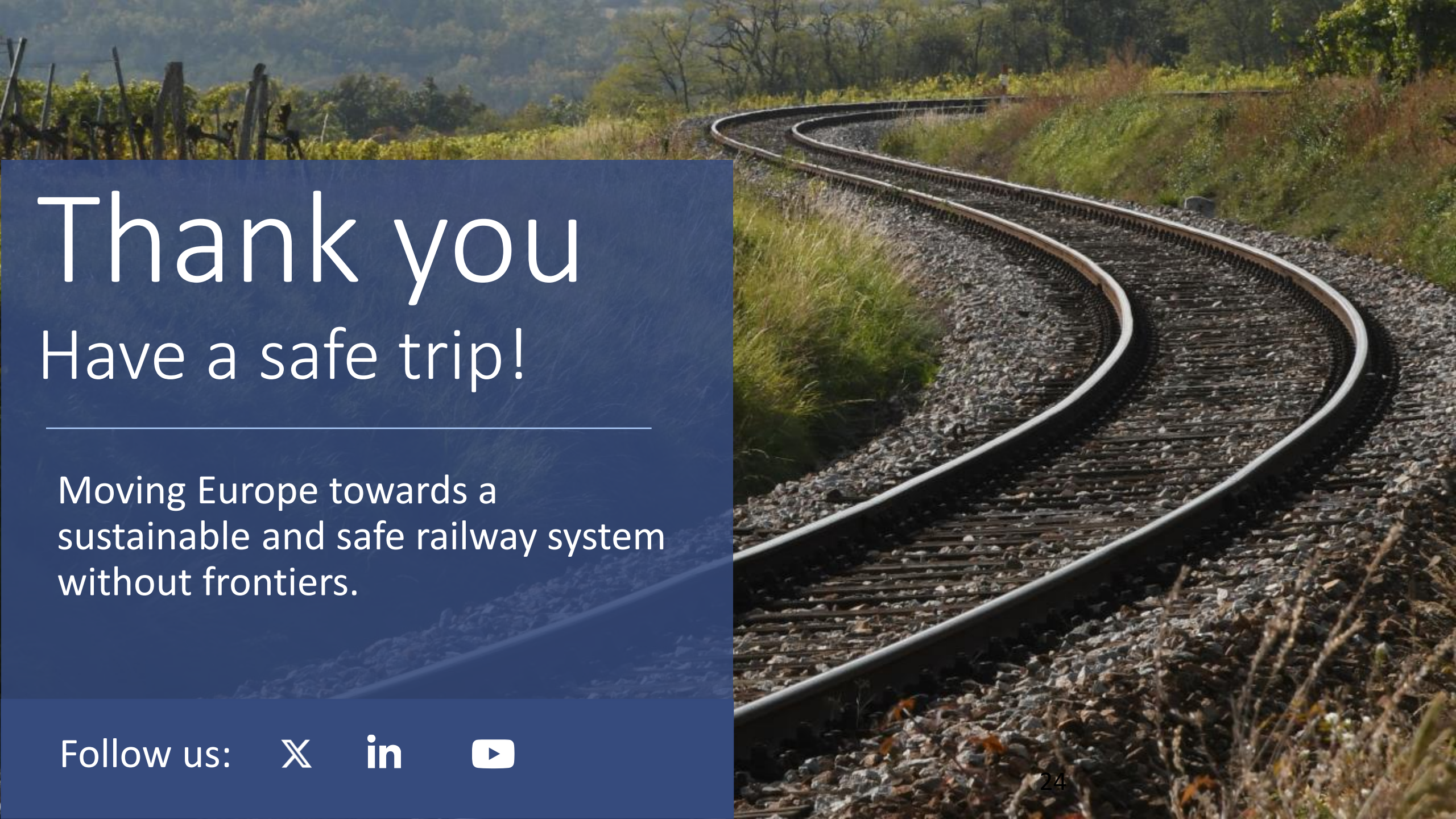
Examples of link to the Safety Culture Model

E1.1 Teamwork and collaboration
E4.1 Leading by example

E1.2 Interpersonal values
F4.3 Decision making

EUROPEAN UNION AGENCY FOR RAILWAYS

- Guide safety culture:
  - https://www.era.europa.eu/activities/safety-culture_en
- Guide TSI OPE:
  - Guide for the application of the TSI OPE (2019 version) (1).pdf
- Guide HOF:
  - https://www.era.europa.eu/activities/safety-management-system/human-and-organisational-factors-hof_en
- Guide CSM on SMS :
  - Guide on safety management system requirements
- General information for Single Safety Certificate applicants:
  - https://www.era.europa.eu/applicants/applications-single-safety-certificates_en



Thank you

Have a safe trip!

Moving Europe towards a sustainable and safe railway system without frontiers.

Follow us: