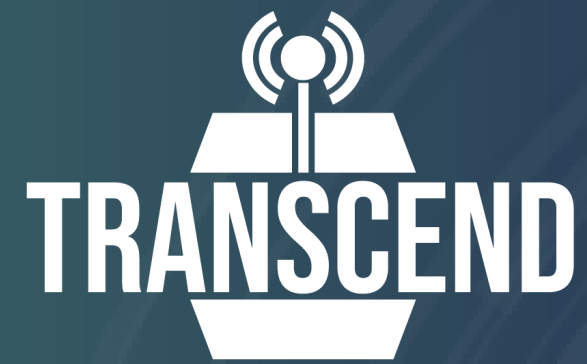




TRANSCEND

Transport Resilience against Cyber and Non-Cyber Events
to prevent Network Disruption

Carolina Cipres, Director of Research
Zaragoza Logistics Center

www.transcend-logistics.eu

*This project has received funding from the European Union's
Horizon Europe research and innovation programme under
grant agreement No 101168023*



**Funded by
the European Union**

Agenda

1. Challenges

2. TRANSCEND ID Card

3. Consortium and pilots

4. Objective

5. Control Tower Concept

6. Approach

7. Expected results

8. Resilience Framework



Challenges

VUCA (Volatility, Uncertainty, Complexity, and Ambiguity)

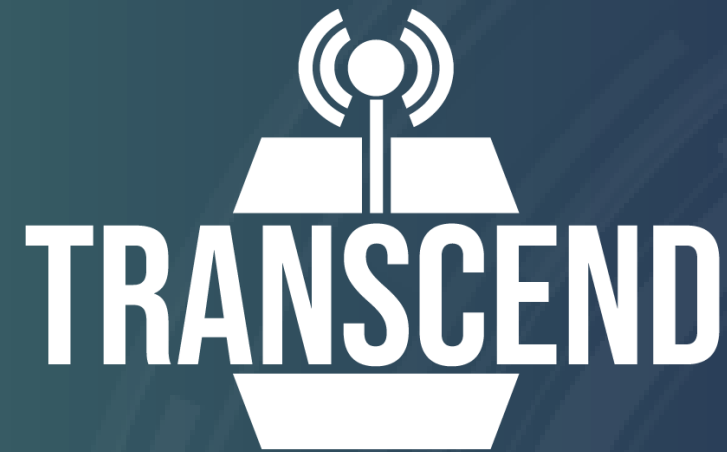
Transport is a highly vulnerable sector

Supply Chain becomes more complex and global

Freight transport increasingly depends on digital systems



ID Card



Transport Resilience against Cyber and Non-Cyber Events to prevent Network Disruption

- Funding tool: HORIZON-CL3-2023-INFRA-01-02
- Topic: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures – Innovation Action
- Duration: 36 months starting on September 1, 2024
- 21 partners
- Budget: around 5M€ (EC contribution: 4.38M€)

www.transcend-logistics.eu

*This project has received funding from the European Union's
Horizon Europe research and innovation programme under
grant agreement No 101168023*



**Funded by
the European Union**



Consortium and pilots

REGULATORY AUTHORITIES



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale



LUXEMBOURG
INSTITUTE OF SCIENCE
AND TECHNOLOGY

LIST



INLAND PORT



RAIL TERMINAL



DBA GROUP



ROAD



TRANSVERSAL

Netcompany

Open ENLCC
European Network of Logistics Competence Centers



Inlecom
Commercial
Pathways

CSP Spain
The Ports for ALL



CSP logitren



CSP Iberian Valencia Terminal S.A.U.



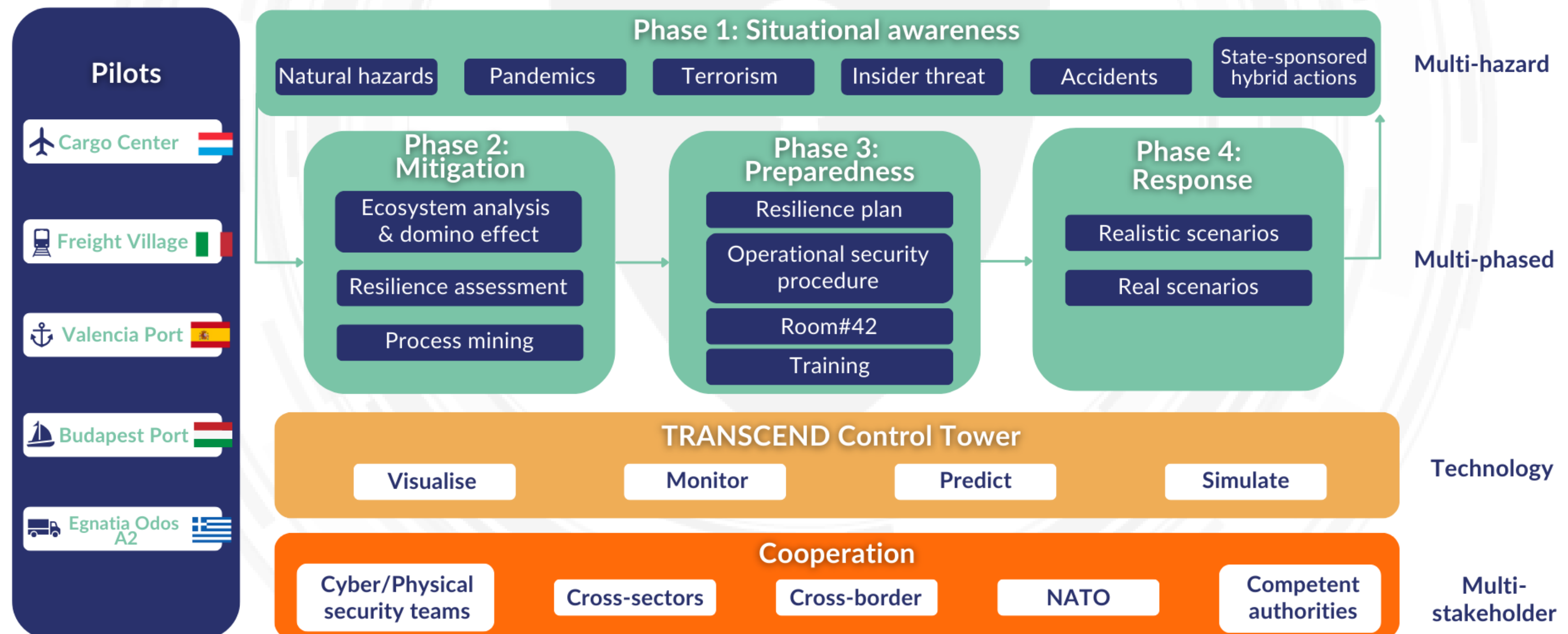
LUXEMBOURG CENTRE
FOR LOGISTICS AND SUPPLY
CHAIN MANAGEMENT (LCL)



MIT GLOBAL
SCALE NETWORK

Focus on Freight Transport

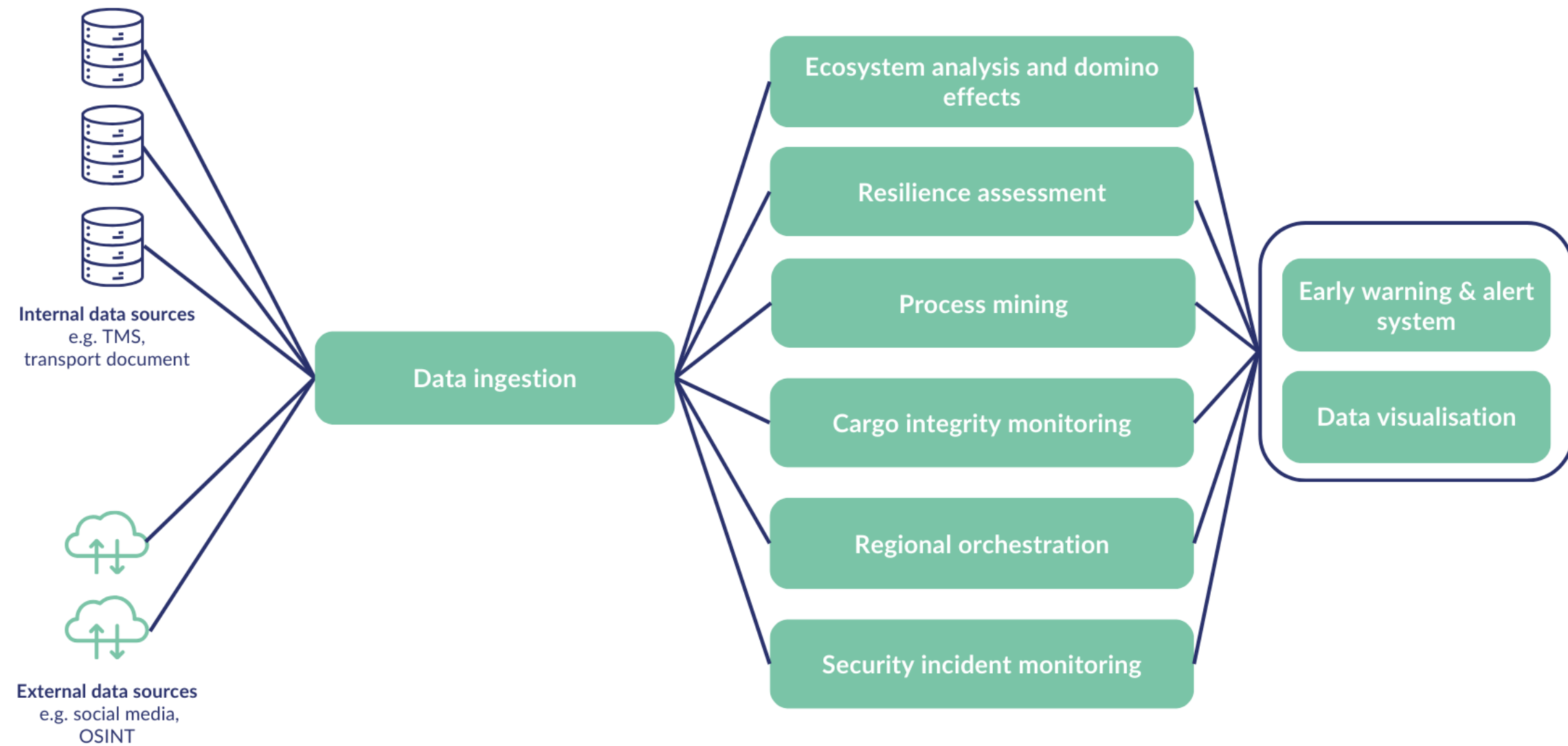
Objective: Provide an integrated set of advanced tools, guidelines and technological solutions to reduce risk, and enhance the protection and resilience of their critical infrastructure and interrelated critical infrastructures against physical, cyber and hybrid threats.



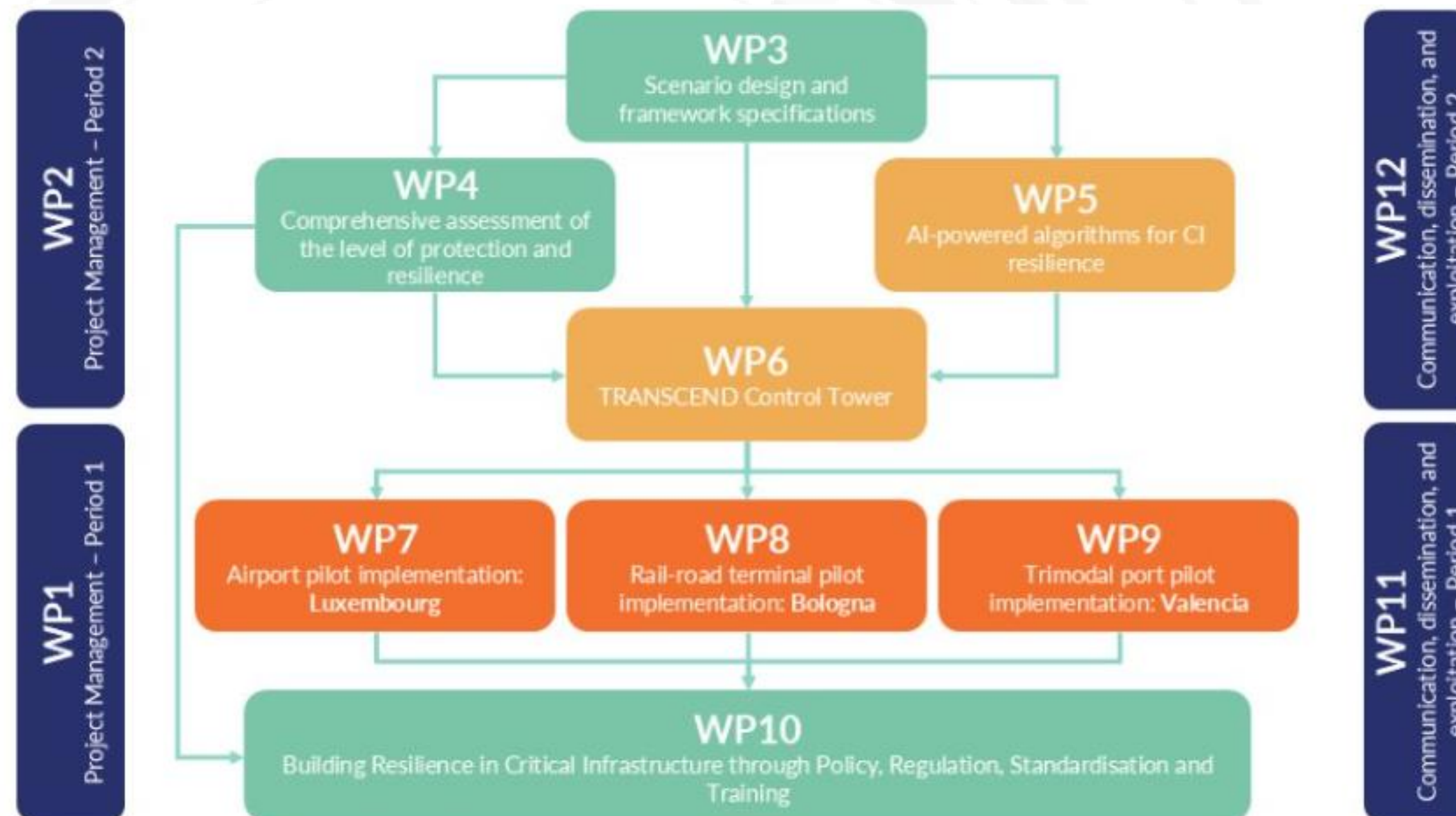
Approach with embedded business intelligence to increase resilience of transport critical infrastructures

To build freight transport resilience by:

- improving transparency
- minimizing risks and exposure to shocks
- building capacity to resist
- absorbing and recovering from disruptive incidents



Work Breakdown Structure (WBS)



+ W13 AI ETHICS

Expected results



IDENTIFIED VULNERABILITIES AND RISKS

*To define mitigation strategies
and improve capacity to
prevent, resist, absorb and
recover from disruptive
incidents*

Vulnerability assessment

Resilience assessment

Process mining analysis

Strengthened cooperation



POLICIES AND PROCEDURES

Guidelines for a resilience plan

Resilience plan for each pilot

Security operational
procedures

Inputs for a national risk
assessment and resilience
strategy



TECHNOLOGICAL SOLUTIONS

*To support implementation of
policies and plans for cost-
effective risk reduction and
resilience*

Machine-readable threat
modelling for large-scale
simulations

State-of-the-art analysis and
experimentation of physical and
cyber detection technologies

ML/AI-based predictive models
and algorithms to detect early
signs of disruption

Generic TRANSCEND Control
Tower



REAL WORLDS PILOTS

*To demonstrate the impacts of
the TRANSCEND solutions to the
freight transport sector*

To secure cargo integrity

To coordinate capacities
between CIs at the regional
level

To monitor security incidents in
multimodal transport

Concept for testing human
behaviour and procedures in
realistic attack scenarios

Resilience Framework



Catalogue of risks

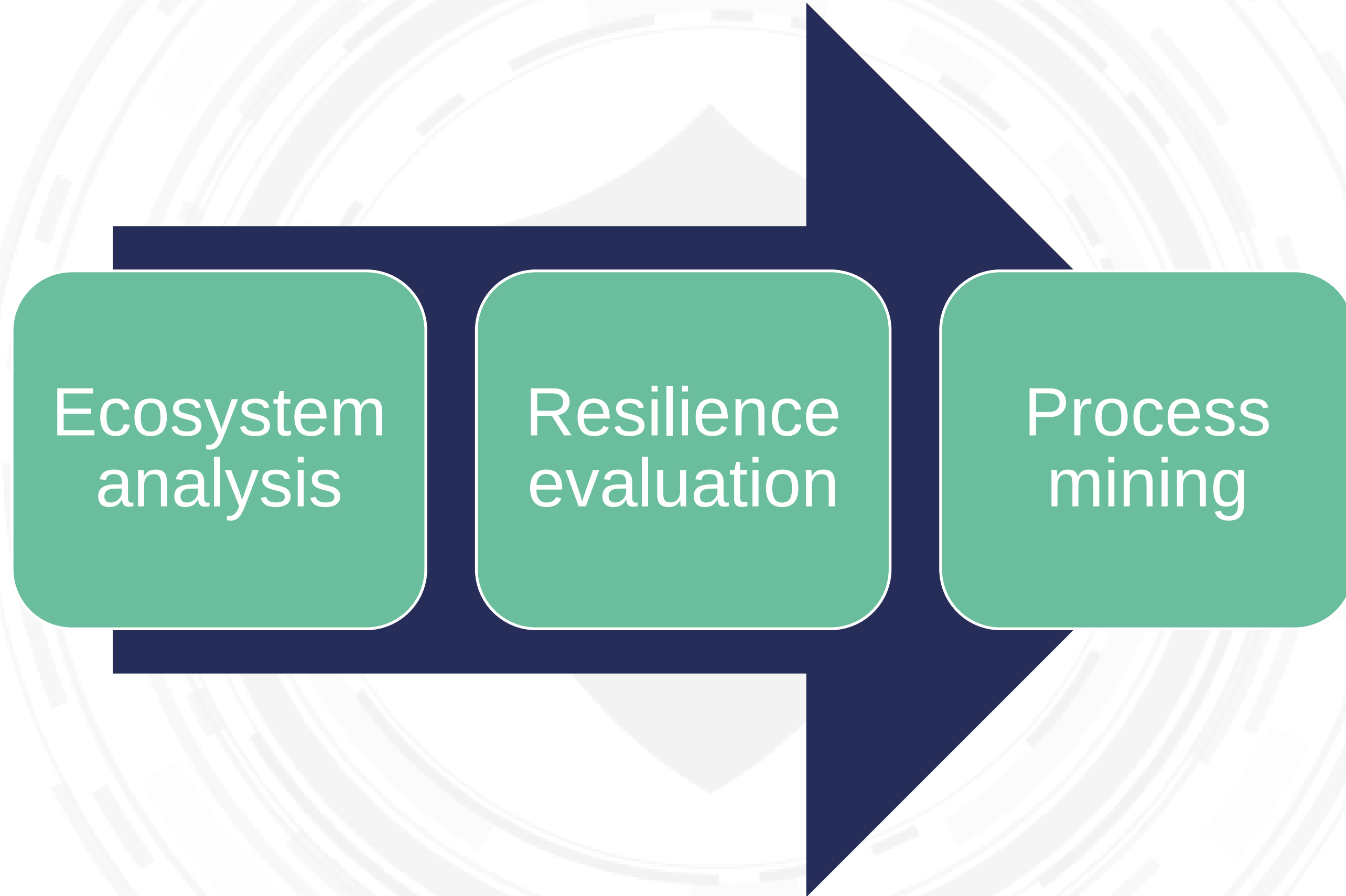
Overview of infrastructure-related risks - physical and cyber threats

Data collection for TRANSCEND use cases

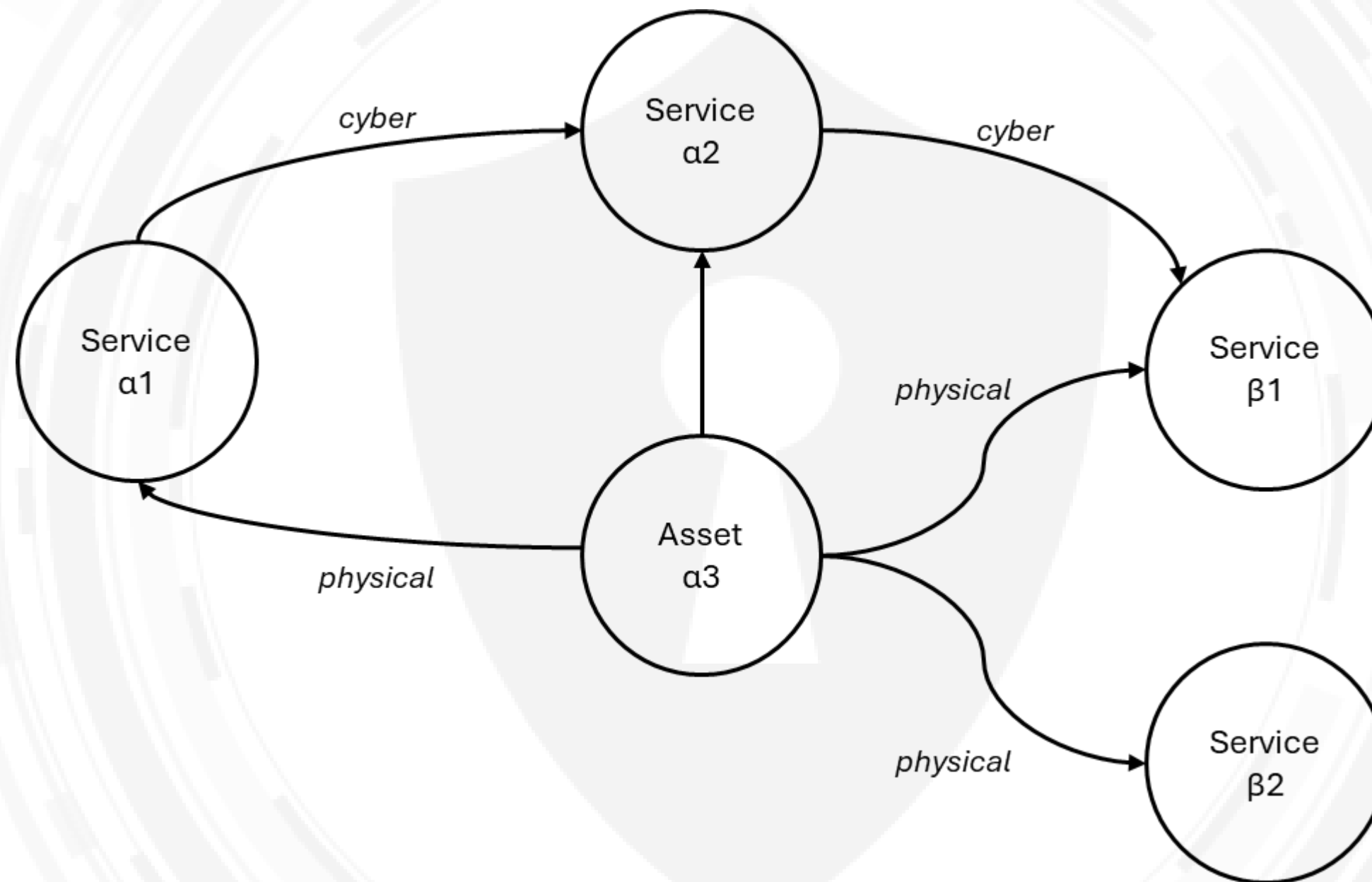
Risk modelling

Scenarios

Resilience framework



The goal is to analyse the ecosystem as a whole and provide the foundations for simulating possible impacts on the resilience of a supply chain composed of several entities (internal or external to the CI) by propagating risk consequences over dependencies (domino effect).



Development of resilience framework:

- Risks identified
- Vulnerabilities
- KPIs/KPP



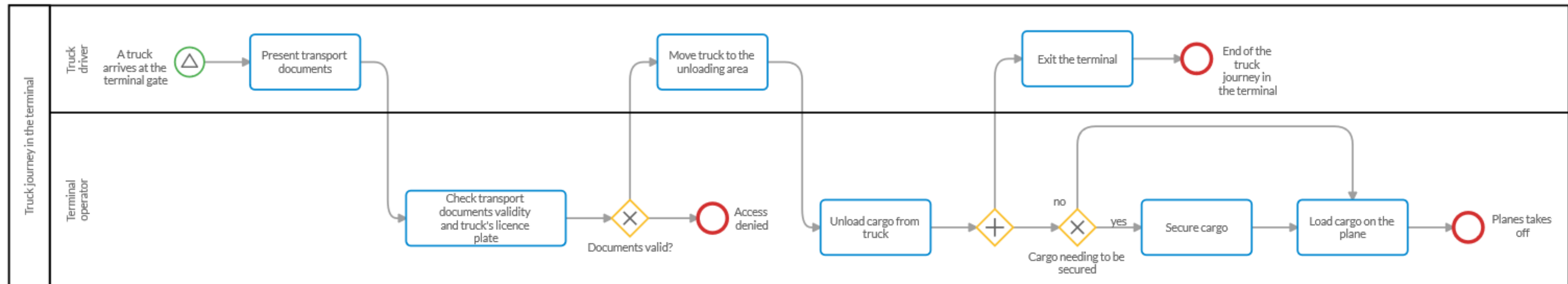
Time to Detect

Time to Recover

Time to Survive

BPMN model with:

- **Root cause insights** to explain why deviations occur
- **Compliance assessment**
- **Recommendations for corrective actions.**
- **A foundation for continuous process improvement**



Next steps: ROOM#42 Exercise

Threat & Attack Vector



- **Risk Sources:** Threat actors (e.g., cybercriminals, hostile insiders), environmental conditions.
- **Events:** The actual incidents (e.g., ransomware attack, physical breach).
- **Consequences:** Disruption of transport services, financial losses, human casualties, reputational damage.
- **Likelihood:** Assessed based on frequency of similar past events and vulnerability.
- **Controls:** Measures to reduce the likelihood or impact (e.g., firewalls, physical barriers, staff training).

The cyberattack
simulation
made in Luxembourg.

What we share with you



- **Catalogue of risks and detection technologies in freight transport**
- **Resilience framework**
- **Pilot reports for Luxembourg, Italy and Spain**
- **Guidelines and lessons learned for a resilience plan**
- **Lessons learned, best practices and replication roadmap**



Thank you!



www.transcend-logistics.eu

 ccipres@zlc.edu.es

 Transcend Project

 TranscendProject