FICHE PROJET

www.list.lu/fr/recherche/projet/transcend/?no_cache=1&cHash=5b580ec9a03be449e3a9955365e9082f

TRANSCEND

TRANSCEND aims to improve the protection and resilience of critical freight transport infrastructure networks across Europe against physical, cyber and hybrid threats, enabling seamless and secure transport operations through a control tower interconnected digital.

Inspiration

The transport network is among the so-called Critical Infrastructures' (CIs), which are essential to maintaining the vital functions of the Single Market. While it is by nature a large-scale interconnected and interdependent system to efficiently move people and goods, its complexity also makes it more vulnerable in the event of a disruption and generates economic impact on a European scale. Due to the increasing cross-border interdependencies between services provided using critical infrastructures in these sectors, an interruption in one Member State may have implications in other Member State or in the Union as a whole. In December 2022, Council Recommendation 2023/C 20/01 suggested giving priority to four of the eleven sectors mentioned in the CER Directive, including transport. Although transport is recognised as a key sector to be protected, freight transport is underrepresented in terms of previous research projects.
As supply chains become more complex and global, they rely more on logistics infrastructures that must be resilient to provide seamless transport. Since freight transport terminals are locations where goods are assembled and dispersed, they have always been a focus of security and safety concerns.
Recent events, such as COVID-19, the blockage of the Suez Canal, the sabotage of the Nord Stream gas pipelines and cyber-attacks on oil ports terminals demonstrate the importance of such CIs for economic systems on a global scale. With the ongoing digital transformation, all management and control processes will increasingly depend on digital systems and processes. This will therefore lead to new types of threats and exposure to hazards due to the need to adapt to these new technologies (e.g. human errors, misconfigurations, failures) on the one hand, and exposure to new forms of cyber-attacks on the other, as already foreseen in the EU's Cybersecurity Strategy and the NIS-2 directive, which aims to modernise the existing legal framework to keep pace with increasing digitisation and an evolving cybersecurity threat landscape.
In conclusion, considering the degree of volatility, uncertainty, complexity and ambiguity (VUCA) associated with the current period of economic and technological transition, it has become crucial for CI operators to be better prepared to prevent, withstand, absorb and recover from incidents, moving from traditional risk management to resilience to ensure business continuity following disruptive events, especially in cases where these cannot be predicted.

Innovation

The overarching objective of TRANSCEND is to provide freight transport critical infrastructure operators with 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. The contributions will be integrated into a Control Tower, a digital platform with embedded business intelligence giving stakeholders a shared and continuous visibility of threats and risks by breaking down silos within and between organisations. To demonstrate the effectiveness of the approach, five diverse CIs will experiment methodological and technological solutions as pilots: three leaders and two followers.

Impact

Expected results:

- Identified vulnerabilities and risks to define mitigation strategies and improve capacity to prevent, resist, absorb and recover from disruptive incidents.
- Policies and procedures including CI resilience plan, security operational procedures and inputs for a national risk assessment and resilience strategy.
- Technological solutions including a generic Control Tower to support implementation of policies and plans for cost-effective risk reduction and resilience.
- Real-world pilots to demonstrate the impacts of the TRANSCEND solutions to the freight transport sector.
- Dissemination and exploitation of results to maximise TRANSCEND impact.

Target communities:

- Critical Infrastructures
- The CI ecosystem includes *freight operators*, *supply chain actors* (manufacturers, shippers and cargo owners) and *other interconnected operators* (e.g. energy providers, emergency services and telecommunication providers).
- Regulators and competent authorities in charge of the national transposition and application of CER and NIS-2 directives.
- Research community and technology providers in the field of freight transport and security.

Partenaires
Luxembourg Institute of Science and Technology (LIST) , Institute for Transport and Logistics Foundation (IT) , Fundación de la comunidad Valenciana para la investigación, promoción y estudios comerciales de Valenciaport (ES) , Fundación Zaragoza Logistics Center (ES) , Netcompany-Intrasoft SA (LU) , European Network of Logistics Competences Centres (BE) , Université du Luxembourg (LU) , Luxembourg House of Cybersecurity (LU) , Interporto Bologna SPA (IT) , Gruber Logistics SPA (IT) , DBA PRO SPA (IT) , Cargolux Airlines International SA (LU) , COSCO Shipping Ports (Spain) Terminals SLU (ES) , CSP Iberian Valencia Terminal Sausa (ES) , CSP Logitren SA (ES) , Inlecom Commercial Pathways Company Limited by Guarantee (IE) , Haut-Commissariat à la protection nationale (LU) , Institut Luxembourgeois de Régulation (LU) , Ministerio del Interior Guardia Civil (SP) , MAHART Container Center Kft (HU) , Egnatia Odos AE (GR)

Support financier
European Commission (EU)

Contact

5, avenue des Hauts-Fourneaux
L-4362 Esch-sur-Alzette
tél : +352 275 888 - 1 | LIST.lu

Cindy GUERLAIN (cindy.guerlain@list.lu)
Jocelyn AUBERT (jocelyn.aubert@list.lu)

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST