AUTOSUP

Preparing the ground for AUTOnomous Multimodal SUPply Chains

Grant Agreement Number: 101147468

2ND ONLINE WEBINAR MEETING MINUTES

12/06/2025

ONLINE

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N. 101147468

Document Summary Information

Acronym	AUTOSUP
Grant Agreement No.	101147468
Meeting ID	T4.2-WEB-2
Date of meeting	**12/06/2025**
Purpose/Title	WEBINAR Meeting Minutes
Location	ONLINE
Distribution	i.e. AUTOSUP Consortium / WP1 participants /…
Minutes taker	[Andreas Kortenhaus (ESC)
Document date	**12/06/2025**

1 Introduction

The second AUTOSUP webinar on "**How can we protect our critical (port) infrastructure to enable safe logistics and trade?**", organized by the European Shippers' Council (ESC) and ALICE, has taken place on 12 June 2025, 13:00 – 15:00h.

The webinar was structured in two main parts with a brief opening speech. The two parts focused on "**Infrastructure in uncertain times**" (2 speakers) and "**The way ahead: safety, security, and resilience of hubs**" (2 speakers).

These minutes first provide the agenda of the webinar, followed by a summary of the key messages of each of the speakers. A list of participants is also available at the end of this document.

2 Agenda

13:00 – 13:10	Opening and AUTOSUP project (Andreas Kortenhaus -ESC)
13:10 – 13:55	Infrastructure in uncertain times
13:10 – 13:25	Driving change & building resilience Ricardo Figueiredo, EU Agency for Cybersecurity, ENISA
13:25 – 13:40	Threats to critical freight transport infrastructure networks across Europe Jocelyn Aubert, EU project TRANSCEND
13:40 – 13:55	Discussion: What are current developments, which risks are present, which are still to come? How safe is automation in hubs? Which regulations are in place and are they sufficient?

13:55 – 14:00	Break
14:00 – 15:00	The way ahead: safety, security, and resilience of hubs
14:00 -14:15	Innovation towards a secure port Joeri Vandeperre, Port of Antwerp-Bruges
14:15 -14:30	A holistic approach to resilience: what can be done and which steps are needed to secure critical infrastructure in hubs? Jan Tore Pedersen, MARLO, EU project SARIL
14:30 -15:00	Discussion: What are future disruptions and how can we prepare for them? Which measures are safe (enough) in the future? Which (EU) regulations do we still need?

3 Opening

Andreas Kortenhaus from the European Shippers' Council (ESC) opened the webinar by briefly introducing the topic and the background of the AUTOSUP project, incl. ESC's involvement and role in the project. The ESC is a European organization representing cargo owners such as manufacturers, retailers, and wholesalers, and they advocate for freight transport interests across Europe. In the AUTOSUP project, ESC leads the policy package, developing EU-level recommendations to support automation in multimodal logistics hubs, addressing regulatory gaps, and considering human, environmental, technological, and security factors.

4 Part 1: Infrastructure in uncertain times

Ricardo Figueiredo from ENISA (European Union Agency for Cybersecurity) provided an overview of the cyber threat landscape, particularly focusing on the transport sector, and discussed relevant EU cybersecurity policies. ENISA, established in 2004 and operating under the 'Cybersecurity Act' (Regulation 2019/881), aims to achieve a high common level of cybersecurity across Europe. Key cyber threats identified from July 2023 to June 2024 include Denial of Service (DoS/DDoS/RDoS) at 41.1% and ransomware at 25.79%. The transport sector accounted for 11% of cyber incidents within this period, making it the second most targeted sector after public administration. The presentation highlighted that the increasing connectivity and transformation of the transport sector from isolated systems to open, connected architectures significantly expand its attack surface. Challenges in maritime cybersecurity include low awareness, the complexity of ICT and SCADA environments, fragmented governance, a lack of holistic approaches, and insufficient economic incentives for implementing strong cybersecurity measures.

The presentation also detailed the EU legislative landscape concerning cybersecurity, with NIS2 (Network and Information Systems Directive 2) being a central pillar. NIS2 focuses on Member State capabilities, risk assessment, and cooperation/information exchange, requiring accountability from top management for non-compliance and mandating security measures and incident notifications for companies. Supply chain security is a critical aspect of NIS2 cyber risk management measures. Primary challenges for NIS2 compliance include vulnerability handling, business continuity, and crisis management, with multi-factor authentication also being a significant concern.

According to the 2024 ENISA NIS Investments report, 89% of organizations will need more staff, especially in technical roles, to meet new EU cybersecurity legislative demands. In 2023, the EU transport sector ranked 6th in median information security spending, marking a 67% increase from the previous year, yet there remains a significant disparity in information security staffing across the sector, indicating uneven capacity to manage cyber risks.

Jocelyn Aubert from LIST (Luxembourg Institute of Science and Technology) introduced the TRANSCEND project focusing on enhancing the resilience of critical freight transport infrastructure networks across Europe against cyber and non-cyber threats. The project, funded by the European Union's Horizon Europe research and innovation program, is a 36-month "Innovation Action" with 21 partners and a budget of approximately €5 million. It aims to provide an integrated set of advanced tools, guidelines, and technological solutions to reduce risks and improve the protection and resilience of critical infrastructure

and interrelated critical infrastructures. The presentation highlights the challenges faced by the transport sector, noting its vulnerability due to its volatile, uncertain, complex, and ambiguous (VUCA) nature, the increasing complexity of global supply chains, and growing dependence on digital systems. Key physical threats identified include climate change, fire, earthquakes, labour shortages/strikes, and physical security breaches. Cyber threats encompass ransomware, data-related threats, malware, phishing/spear phishing, breaches/intrusions, credential harvesting, Denial of Service (DoS/DDoS/RDoS), spoofing, supply chain attacks, and vulnerability exploitation.

The TRANSCEND project's approach involves a multi-phased strategy that includes situational awareness, mitigation, preparedness, and response, all underpinned by a "TRANSCEND Control Tower" concept. This control tower aims to build freight transport resilience by improving transparency, minimizing risks, building capacity to resist, and absorbing and recovering from disruptive incidents. The project seeks to achieve this through ecosystem analysis and domino effect simulations, resilience assessments (measuring Mean Time to Detected Failure, Time to Survive, and Time to Recover), process mining for real-time analysis and threat simulation, cargo integrity monitoring, regional orchestration, and security incident monitoring. The consortium involves various partners, including cargo centers, rail terminals, maritime ports, inland ports, and regulatory authorities, demonstrating a multi-stakeholder and cross-sectoral cooperation model.

5 Part 2: The way ahead: safety, security, and resilience of hubs

Joeri Vandeperre from the Port of Antwerp-Bruges presented the implementation of an innovative security vision based on four building blocks: localization, authorization, identification, and signalization, utilizing a "digital nervous system" with various sensor devices. A key realization of this vision is the D-HIVE network of automated drones, which has been operational since 2018. This network allows for 18 flights a day, 24/7, with authorization to fly beyond visual line of sight (BVLOS) over water. A central coordination and control center manages these drones, and communication occurs via a dedicated 5G network. The port also uses drone detection systems to identify unauthorized flights, recording details like drone model, altitude, speed, coordinates, and operator ID.

Beyond drones, the port's security measures include a comprehensive license plate camera network, acting as a "shield" around the port with 28 measure points and 64 cameras, with plans for further densification. There is also a central control room integrating camera networks from the Port of Zeebrugge, including both port authority and tenant perimeter cameras. The port leverages data for security, including automatic object detection from aerial and satellite images, and analyzing nonregistered voyages to identify potential illegal activities like degassing or suspicious trafficking. The fiber network itself is being transformed into a 170 km sensor. Furthermore, the "Certified Pick up" (CPu) flow for container pick-ups has over 1,000,000 containers picked up, with a small percentage blocked due to customs issues, invalid Alfapasses, or lack of release rights. These initiatives aim to ensure business continuity and a virtually secured port.

Jan Tore Pedersen from MARLO presented the SARIL project (Smart sAfe Resilient Infrastructures for Logistics) which is a project aiming to enhance the resilience and safety of critical logistics infrastructures

and their supply chains against both cyber and physical threats. The project addresses the increasing complexity of logistics infrastructure, which has become more interconnected and dependent on digital systems, making it vulnerable to various threats. SARIL's primary objective is to develop a security and resilience framework and a "system of systems" that will empower logistics infrastructure operators to achieve continuous resilience, improve their security posture, and enhance business continuity. This is achieved through a multi-faceted approach including risk identification, threat anticipation, real-time detection, and rapid recovery capabilities. The project is aligned with EU policies like NIS2 and CER, emphasizing the need for robust cybersecurity and resilience measures in critical sectors.

The SARIL framework focuses on several key areas to build resilience. It incorporates real-time threat intelligence through multi-source data ingestion, enabling advanced analytics for comprehensive threat detection and assessment. A crucial aspect is the development of a resilience assessment methodology that quantifies risk and assesses an organization's capacity to withstand and recover from disruptive events. The project also emphasizes the importance of secure data exchange and communication to protect sensitive information across the supply chain. Through pilots in real-world scenarios, such as the Port of Barcelona and the Ports of Genoa, SARIL aims to validate its solutions and provide a holistic approach to managing risks and ensuring the continuity of logistics operations.

SARIL aims to provide a comprehensive suite of tools and methodologies including an overarching security and resilience governance framework, a collaborative risk assessment platform, and operational continuity and crisis management tools. By integrating diverse data sources and applying advanced analytical techniques, SARIL seeks to offer early warning signals and enable proactive decision-making for logistics operators. The project’s outcomes are expected to contribute to safer, more efficient, and resilient logistics and transport operations across Europe, ultimately fostering digital trust and security within the critical infrastructure landscape.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N. 101147468Funded by the European Union. Views and opinions expressed are however those of the autor(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.