SharePort: Enhancing Resilience of Maritime Port Infrastructures through Trustworthy Resource Sharing

1st Middelbeck, Gabriela
BIBA - Bremer Institut für Produktion und Logistik GmbH at the University of Bremen, Germany
University of Bremen, Faculty of Production Engineering
Bremen, Germany
gabichim@uni-bremen.de

2th Majri, Sarra
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany,
sarra.majri@dlr.de

3rd Fischer, Lars
Hochschule Bremerhaven
Bremerhaven, Germany
lars.fischer@hs-bremerhaven.de

4th Hutter, Dieter
German Research Center for Artificial Intelligence
Bremen, Germany,
dieter.hutter@dfki.de

5th Schaefer, Manuel
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany,
manuel.schaefer@dlr.de

6st Teucke, Michael
BIBA - Bremer Institut für Produktion und Logistik GmbH at the University of Bremen, Germany
Bremen, Germany
tck@biba.uni-bremen.de

7th Stockbruegger, Jan
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany
jan.stockbruegger@dlr.de

8th Freitag, Michael
BIBA - Bremer Institut für Produktion und Logistik GmbH at the University of Bremen, Germany
University of Bremen, Faculty of Production Engineering
Bremen, Germany
fre@biba.uni-bremen.de

***Abstract*—Maritime ports are critical infrastructures whose performance and reliability are essential for global supply chains. However, the resilience of port operations is under pressure due to an increasing risk of disruption caused by geopolitical tensions, climate-related events, labor shortages and technical failures. Although cooperation between port operators has the potential to help overcome local disruptions, concerns about data confidentiality and competitive pressures often hinder progress. In this paper we present SharePort, an ongoing interdisciplinary research project investigating how secure, trust aware resource sharing among port actors can enhance the resilience of maritime port infrastructure. We combine organizational, technological and security-oriented approaches to enable the temporary sharing of underutilized resources, such as equipment or storage capacities, while respecting sovereignty, confidentiality and heterogeneous trust relationships. The approach follows a community-based methodology that integrates stakeholder consultation, the formal modeling of sharing structures, the design of security policies, and a simulation game for evaluation purposes. A resilience assessment framework will be developed to analyze the impact of resource sharing under defined disruption scenarios.**

Keywords—Maritime resilience, critical infrastructure, port security, resource sharing, coopetitive systems

I. Introduction

Maritime ports represent central nodes in global logistics networks and are increasingly recognized as critical infrastructures [1], [2], [3]. Their complex socio-technical nature—characterized by interdependencies between operators, terminals, logistics service providers, authorities, and IT systems—makes them particularly vulnerable to disruptions [4]. Recent events have demonstrated that even localized failures can propagate through supply chains, causing significant economic and societal impacts [1], [5].

Resilience has therefore become a key objective in maritime research and policy [3]. Beyond technical robustness, resilient port systems require organizational adaptability, cooperative governance structures, and secure information exchange [6][2]. By enabling port operators to access underused resources on a temporary basis, such arrangements could enhance the resilience of port operators by increasing operational flexibility and reducing vulnerability to capacity shortages. However, port actors often operate in competitive environments and are reluctant to share resources or operational data due to concerns regarding intellectual property, security, and loss of autonomy [7].

Against this background, the authors investigate whether and how secure, temporary resource sharing among port stakeholders can improve the ability of ports to absorb, respond to, and recover from disruptions. The project SharePort explicitly addresses resilience and security as intertwined challenges and aligns closely with current research on critical maritime infrastructure protection.

II. RELATED WORK

Sharing economy has gained considerable traction in recent years proposing the dissemination of a wide variety of resources [8], [9]. The term 'resource' is open to interpretation, with varying definitions depending on the discipline and level of consideration. In essence, any material or immaterial entity that possesses a value-adding characteristic can be designated as a resource. From a production technology perspective, both technical objects, such as machines or transport units, and spatial capacities are considered resources [10]. The fundamental principle underpinning the sharing economy is that resources within the sharing network are made available for temporary use or can be used temporarily and on loan [11] [9]. Initial examples of industrial resource sharing can be found in the form of freight exchanges or the shared use of storage space [12]. Furthermore, this format offers a wide range of other implementation options, including in the area of seaports.

The current literature considers resource sharing as a key way of increasing the profitability of container ports, covering a wide range of materials, infrastructure and even human resources [13]. Maritime infrastructures are critical infrastructures for they play a crucial role in supplying a society, the functioning of the economy, maintaining mobility and the deployment of renewable energies. The Maritime Resilience Breakthroughs define resilient maritime sectors as ones "that are equipped to withstand and adapt to changing conditions and recover positively from shocks and stresses, whether they be related to climate hazards, geopolitical uncertainty, technological change, decarbonisation efforts, or other unforeseen disruptors" [14].

Existing research on maritime resilience emphasizes the need for redundancy, robustness, and recovery capabilities of port infrastructures [3], [15] and, in particular, highlight coopetition to enhance resilience in the maritime sector [2], [16]. [17] suggests collaboration in the maritime industry around shared projects generating collective values, like an increased port resilience. This collaboration is characterized by complex relationships in which cooperation coexists with competition, reflecting the coopetition dynamic [17].

The more maritime systems and their interplay are managed and organized in a digital way, the more IT-security and privacy become eminent issues for a resilient maritime ecosystem. Its distributed nature prevents the use of traditional perimeter-based security policies and paves the way for zero-trust policies checking, as a matter of principle, everything for authenticity before using it [18]. Data or "intellectual property" (IP) respectively has become a main assert for stakeholders and joint operations are always compromises between the added values provided by cooperation and the caused (potential) disclosure of sensitive data [18]. Advances in multi-party security protocols now allow individual data to be compared or processed jointly without the need for a trusted third party or for disclosing the partners the individual source data, and thus, reduces the barriers to form new cooperations [19].

Our approach combines these strands to create a concept for resilient and secure port operations. The practical impact of SharePort is to strengthen the resilience of maritime ports through a coopetitive approach. The study aims at developing a conceptual framework for resource sharing among port actors, while ensuring security and trust among stakeholders.

III. METHODOLOGICAL APPROACH

Our conceptual framework for resource sharing within stakeholders of a port combines the following aspects.

A. Stakeholder analysis

Container ports usually consist of several terminals and a wide range of stakeholders, each pursuing distinct economic and strategic interests. Their competitive nature often leads to local rather than system-wide optimization, although overall port performance depends on effective coordination and alignment of these interests.

The engagement of stakeholders is twofold: The first objective is to identify their specific requirements and constraints for implementing resource sharing in ports. The study assesses opportunities and risks, examining the transferability of resource-sharing concepts to the port context. Requirements are derived through interviews and workshops, following a voice-of-the-customer approach. The second objective is to evaluate the prototype of the platform against the previously specified requirements. The evaluation of the platform will be performed with the help of a game, that simulates a resource sharing scenario in a port.

B. Resources for sharing

Port operations rely on a wide range of resources, including handling equipment, transport vehicles, digital infrastructure, storage capacities, and specialised human expertise. These resources differ significantly in terms of ownership, utilisation rates, operational criticality, mobility, and regulatory constraints.

Before developing a resource-sharing concept, a systematic classification and evaluation of these assets is required, as not all resources are equally suitable for shared use. Therefore, the authors conducted a structured assessment focusing on technical feasibility, operational flexibility, economic viability, and governance implications. Based on this evaluation, appropriate resource categories were selected, as shown in Table 1.

TABLE I. OVERVIEW OF POSSIBLE RESOURCES FOR SHARING

Resource type	**Example**
Yard space	Container storage yards; empty container depots; temporary overflow areas; cross-docking zones
Warehousing facilities	Bonded warehouses; cold storage facilities; hazardous goods storage; consolidation centres
Mobile handling equipment	Reach stackers; forklifts; straddle carriers; terminal tractors
Transport assets	Shuttle trucks; rail wagons; barges; chassis pools
Specialized handling equipment	Mobile harbour cranes; heavy-lift cranes; bulk handling systems; automated guided vehicles (AGVs)
Digital resources	Cybersecurity infrastructure; data hubs; port community systems

C. Disruption scenarios

Demand for shared resources may arise from temporary capacity shortages, particularly in the context of operational disruption scenarios. Such disturbances may include unexpected equipment breakdowns, supply chain interruptions, labor shortages or other unforeseen events that limit the availability of a company's own resources. Short-term peak demand can create capacity bottlenecks. Resource sharing is also relevant when assets are needed only temporarily (e.g., for one-off projects) or are chronically underutilized. In such cases, shared use represents a more economically efficient solution (e.g., snow-clearing vehicles). Table 2 outlines potential disruption scenarios for ports that may lead to a need for resource sharing.

TABLE II. OVERVIEW OF POSSIBLE DISRUPTION AND THEIR RELEVANCE FOR SHARED RESOURCES

Disruption Scenario	**Example**	**Relevance for Resource-Sharing**
Technical failure	Breakdown of cranes, gate systems or conveyor belts	Shared forklifts, or transport vehicles from neighboring terminals can compensate for the failure and maintain cargo handling operations
Natural hazards / environmental events	Storms, flooding, or ice affecting terminal infrastructure	Shared storage areas, equipment or alternative terminals can enable continued operations and reduce downtime
Intentional disruptions	Blockage of terminal access or manipulation of critical infrastructure	Shared terminal capacities or rerouting to partner terminals ensure continuity of logistics operations

The overview shows not only possible scenarios in which resource sharing can support the resilience of a port but also illustrates that disruptions can be differentiated based on their origin and characteristics.

D. Resource-sharing platform

The proposed resource-sharing mechanism is implemented via a centralized digital platform that coordinates access, allocation, and governance of shared assets. This intermediary infrastructure enhances transparency and standardizes transaction processes among port stakeholders.

The resource sharing platform should reflect the dual role of port operators as both providers and users of shared resources. In this context, the authors examine the requirements for such a platform from the perspective of port operators, both functional and non-functional. The functional requirements delineate the fundamental operational capabilities of the platform, encompassing resource listing, booking and allocation mechanisms, user management, contract handling, and monitoring of usage. The non-functional requirements encompass quality attributes such as security, data protection, interoperability with existing terminal and port systems, scalability, reliability, and performance efficiency.

E. Security infrastructure

Ensuring the long-term use of a resource-sharing platform requires a high level of trust by the participants in the integrity and accuracy of information as well as the confidentiality of interactions and internal state of participants. A significant concern for sharing in the business-to-business sector pertains to the potential disclosure of sensitive data to competitors. Consequently, requirements pertaining to security, privacy, and information flow control [20] need to be identified, modelled, and enforced within the envisaged shared-resource system. The acceptance and trustworthiness of such a system are contingent upon the assurance that confidential operational data will not be disclosed to unauthorised parties, that procedural mechanisms will not disadvantage or impede any actors, and that system processes will remain transparent, verifiable, and resilient against external and internal attacks. Conflicts between transparency and confidentiality requirements have to be addressed.

Primary internal threat actors are entities with legitimate access to the platform. The category "Competitor" from the Threat Agent Library [21] covers coopetitors from the harbor community. These actors primarily threaten Availability with respect to resources or Confidentiality of operational data. External threat agents considered aim at damage caused by disruption of service. Most likely categories are Government Cyberwarrior or Terrorists. While the former category calls for elaborate privacy techniques, the latter has to consider advanced and persistent threat activities.

Trust and acceptance depend critically on safeguarding confidential operational data, preventing discriminatory or obstructive procedures, and ensuring that system processes remain transparent, auditable and resilient to external and internal attacks. Aggregation of different facets of trust, e.g. as given in [22] can be used to consolidate the security facet into the overall evaluation. A carefully designed security infrastructure will provide a central anchor of trust that enables efficient and trustworthy coopetition. This central infrastructure will be based on a combination of established security mechanisms, such as role-based access control schemes, privacy preserving measures and cryptographic protocols to consistently enforce the security policy derived from the results of our stakeholder consultations. Security provides only one crucial facet that influences the trustworthiness of the system.

F. Resilience

The overarching objective of this study is to investigate how resource sharing can enhance the resilience of critical infrastructures, such as seaports. A key performance dimension in this context is the continuity of essential services, for instance container handling operations. To address this, an assessment framework for measuring port resilience needs to be developed. This framework has to integrate technical, organisational and human factors and derive resilience indicators that enable continuous assessment of both short-term responsiveness and long-term impacts on port operations.

IV. CONCLUSION

By addressing resilience and security jointly, the authors aim to respond to key challenges in protecting critical maritime infrastructures by developing a resource sharing concept for ports. For practice, it provides actionable guidance for port communities seeking to enhance resilience without compromising competitive or security interests.

Beyond company-level benefits, resource sharing strengthens overall port resilience by mitigating short-term shortages and disruptions (e.g., equipment failures or demand fluctuations). The project demonstrates that cooperation and competition can coexist under appropriate governance and technological safeguards. By integrating stakeholders' engagement, security-by-design, and resilience assessment, it offers a holistic approach to safeguard critical maritime infrastructures. Following the successful development of the concept and its testing in a simulation game, the project will focus on investigating practical feasibility and the possibilities for transfer to real-world application contexts.

V. OUTLOOK

The proposed approach and platform concept constitute an initial step toward structured resource sharing in port environments and require further empirical validation and refinement. Future research should expand and validate the identified functional and non-functional requirements by incorporating additional stakeholder perspectives.

A simulation-based serious game or structured scenario exercise is recommended to test stakeholder behavior in prototypical disruption situations and to analyze cooperation incentives and potential barriers. Furthermore, pilot testing of the platform is necessary to assess technical feasibility, usability and interoperability with existing systems. Port stakeholders are invited to actively participate in this process. Early involvement enables companies to integrate their specific requirements, shape the platform's development and benefit from potential efficiency and resilience gains.

Acknowledgment

This work was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) as part of the community project 03DPC1812A „Resilient Smartport: Enhancing Supply Chain Robustness through Dynamic Resource Sharing“ within the DATIpilot innovation community SPorT.

References

[1] G. T. Tsoulfas, "Port resilience: a systematic literature review," *Marit Econ Logist*, 2025, doi: 10.1057/s41278-025-00326-3.
[2] W. Li, A. Asadabadi, and E. Miller-Hooks, "Enhancing resilience through port coalitions in maritime freight networks," *Transportation Research Part A: Policy and Practice*, vol. 157, pp. 1–23, 2022, doi: 10.1016/j.tra.2022.01.015.
[3] Y.-Y. Lau, Q. Chen, M. C.-P. Poo, A. K. Ng, and C. C. Ying, "Maritime transport resilience: A systematic literature review on the current state of the art, research agenda and future research directions," *Ocean & coastal management*, vol. 251, p. 107086, 2024, doi: 10.1016/j.ocecoaman.2024.107086.
[4] J. Verschuur, E. E. Koks, and J. W. Hall, "Ports' criticality in international trade and global supply-chains," *Nature communications*, early access. doi: 10.1038/s41467-022-32070-0.
[5] R. Panahi, N. Sadeghi Gargari, Y.-Y. Lau, and A. K. Y. Ng, "Developing a resilience assessment model for critical infrastructures: The case of port in tackling the impacts posed by the Covid-19 pandemic," *Ocean & coastal management*, early access. doi: 10.1016/j.ocecoaman.2022.106240.
[6] T. Brandt, D. Hutter, C. Maeder, and R. Müller, "Towards a Secure and Reliable IT-Ecosystem in Seaports," 29th Conference of the International Association of Maritime Economists, 2021. [Online]. Available: https://arxiv.org/pdf/2111.13436
[7] D.-W. Song, "Port co-opetition in concept and practice," *Maritime Policy & Management*, vol. 30, no. 1, pp. 29–44, 2003, doi: 10.1080/0308883032000051612.
[8] R. Laurenti, J. Singh, J. M. Cotrim, M. Toni, and R. Sinha, "Characterizing the Sharing Economy State of the Research: A Systematic Map," *Sustainability*, vol. 11, no. 20, p. 5729, 2019, doi: 10.3390/su11205729.
[9] M. Freitag and D. Lappe, "Perspektiven von Shared Resources in der Produktion: Eine Analogie zwischen Web 2.0 und Industrie 4.0 als Basis für gemeinsam genutzte Ressourcen," *Industrie 4.0 Management*, vol. 31 (4): 39–42, 2015.
[10] K. von dem Berge, U. Juttner-Schlange, and S. Maklan, Eds., *Resource sharing in business-to-business contexts: a conceptualisation and guide for future research*, 2022.
[11] M. Freitag, T. Becker, and N. A. Duffie, "Dynamics of resource sharing in production networks," *CIRP Annals*, vol. 64, no. 1, pp. 435–438, 2015, doi: 10.1016/j.cirp.2015.04.124.
[12] A. A. H. Haqqani, A. Elomri, and L. Kerbache, "Sharing Economy: A Systematic Review of Definitions, Drivers, Applications, Industry status and Business models," *IFAC-PapersOnLine*, vol. 55, no. 10, pp. 490–495, 2022, doi: 10.1016/j.ifacol.2022.09.441.
[13] X. Jin, K. T. Park, and K. H. Kim, "Storage space sharing among container handling companies," *Transportation Research Part E: Logistics and Transportation Review*, vol. 127, pp. 111–131, 2019, doi: 10.1016/j.tre.2019.05.001.
[14] "The Maritime resilience breakthroughs," [Online]. Available: https://www.climatechampions.net/media/dirpvrah/maritimeresiliencebreakthroughs.pdf
[15] H. Chen, J. S. L. Lam, and N. Liu, "Strategic investment in enhancing port–hinterland container transportation network resilience: A network game theory approach," *Transportation Research Part B: Methodological*, vol. 111, pp. 83–112, 2018, doi: 10.1016/j.trb.2018.03.004.
[16] A. Khaslavskaya, J. Monios, and V. Roso, "Using coopetition to increase asset utilization and market coverage of dry ports," *Research in Transportation Business & Management*, vol. 57, p. 101219, 2024, doi: 10.1016/j.rtbm.2024.101219.
[17] A. N. Andriamanantena, B. Laperche, and S. Boutillier, "Building Circular Innovation Ecosystem in Industrial Port Territories: The Case of Dunkirk, France," in *Business Models for the Circular Economy* (Sustainability and Innovation), V. Prokop, J. Stejskal, J. Horbach, and W. Gerstlberger, Eds., Cham: Springer International Publishing, 2022, pp. 139–167.
[18] J. Pennekamp *et al.*, "An Interdisciplinary Survey on Information Flows in Supply Chains," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–38, 2024. doi: 10.1145/3606693. [Online]. Available: https://dl.acm.org/doi/10.1145/3606693
[19] J. Pennekamp *et al.*, "Offering Two-way Privacy for Evolved Purchase Inquiries," *ACM Transactions on Internet Technology*, vol. 23, no. 4, pp. 1–32, 2023. doi: 10.1145/3599968. [Online]. Available: https://dl.acm.org/doi/10.1145/3599968
[20] Thomas Bauereiß, Dieter Hutter, and Heiko Mantel, "Information Flow Control for Workflow Management Systems," *IT - information technology (IT)*, vol. 6/2014, pp. 294–299, 2014.
[21] T. Casey, "Threat Agent Library Helps Identify Information Security Risks," 2007, doi: 10.13140/RG.2.2.30094.46406.
[22] B. Siemers, L. Fischer, and S. Lehnhoff, "A Trust Model in Control Systems to Enhance and Support Cybersecurity," in *2022 IEEE 7th International Energy Conference (ENERGYCON)*, Riga, Latvia, 2022, pp. 1–6, doi: 10.1109/ENERGYCON53164.2022.9830327.