Economics & Business Management
ISSN Print: 3079-5214
ISSN Online: 3079-5222
https://doi.org/10.63313/EBM.9201

Profit vs. Risks: The Mechanisms Behind Paralysis Risks and Core Impacts of Highly Automated Ports

Chennuo Wan[1,*]. Zhenxi Chen[2] and Zihe Chen[2]
[1]Hangzhou Foreign Languages School Cambridge A-Level Center, Hangzhou, China
[2]High School Affiliated to Shanghai Jiaotong University IB Centre, Shanghai, China
Email: 18868860716@163.com

How to cite this paper: Wan, C., Chen, Z., & Chen, Z. (2026). Profit vs. risks: The mechanisms behind paralysis risks and core impacts of highly automated ports. Economics & Business Management, 6(2), 1–9. ISSN Print: 3079-5214, ISSN Online: 3079-5222.
https://doi.org/10.63313/EBM.9201
Published: 2026-07-06

Copyright © 2026 by author(s) and Erytis Publishing Limited.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Abstract

This paper takes DP World as an example to analyze the paralysis risks, their mechanisms, and core impacts that highly automated ports face in the pursuit of profit maximization, and proposes corresponding strategies at the institutional and national levels. Under the assumption of profit maximization, private ports overly emphasize the reduction of explicit costs and promote the economies of scale brought about by automation, while underestimating implicit costs and related risks. As shown by the case analysis of DP World, its profit-driven promotion of automation ultimately led to losses during a cyberattack. The proposed suggestions at the institutional and national levels can effectively balance automation efficiency and operational risks. However, this study has limitations. The framework is only applicable to private ports and does not consider the impacts of government-led ports and differences in regional economic development levels on the automation effects and reasonable levels.

Keywords

Highly Automated Ports; Paralysis Risks; Profit Maximization; DP World; Cyber-Attack; Implicit Costs; Operational Risk Management

I. Introduction

AI (Artificial Intelligence) technology in all industries is a double-edged sword; it brings higher efficiency and lower costs to businesses while having underlying problems for those who overuse it. Everyone knows there should be a limit: don't rely on automation too much. Yet driven by profit maximisation [7](Keen S, 2006), firms tend to focus only on reducing costs and realizing economies of scale that drive down average costs, so the invisible risks that are also brought by AI may be overlooked. Even when companies know there is an "optimal" level of automation, information asymmetry and the lack of dynamic measurement methods make it nearly impossible to stop at the optimal value. This essay conducts an analysis using DP World as an example: Its BOXBAY system has increased efficiency by 31% and reduced energy consumption by 29%. However, due to 98% of its supply chain

relying on the AI system, a single cyber attack which paralyzed the BOXBAY system caused approximately $21.2 million in losses within just three days. According to the report, DP World's investment in cybersecurity amounts to $90 million, far exceeding the $7.8 million upper limit suggested by the Gordon-Lobb model.

The essay therefore proposes a plan that combines multiple strategies on institutional and national dimensions. At the institutional level: Enterprises should establish human labour backup systems, control safety investment within 37% of the expected losses according to the Gordon-Loeb model, and be willing to abandon sunk costs. At the national level: The government should implement hierarchical supervision, require ports to disclose the proportion of sunk costs on a quarterly basis, and mandate that risk assessments be completed before major system upgrades.

However, looking forward, firms and individuals should not overly rely on this single theoretical model. The application scenarios of AI are constantly evolving, and the calculation of the optimal safety investment level will not remain the same. People should calculate the optimal value frequently according to technological changes and the diversity of business operations. On the other hand, enterprises themselves also need to learn to abandon sunk costs or only focus on maximizing profits while neglecting safety guarantees. We expect enterprises to pursue maximum profits within a reasonable risk framework.

II. Problem Statement

Since the first automated container port was launched in Europe in the 1990s, port automation has spread across the global maritime industry. Today, nearly 40 ports that are partly or fully automated are in operation around the world, and this process is expected to speed up in the next five years. It is estimated that investment in these projects will increase by $10-$15 billion [9] (ITF, 2021). These numbers show that automation has become a main development strategy for international ports.

As the degree of automation in ports increases, an important economic issue emerges. Automation may bring higher efficiency, lower labor costs, and a competitive advantage to port terminal owners. However, excessive reliance on automated systems makes ports vulnerable to operational and technical risks. For example, for some highly automated parts, if the core system fails, it will lead to a series of chain reactions, including possible problems such as port paralysis, significantly prolonged import detention time, data leakage, and direct economic losses. This article examines the issue of port automation from the perspectives of efficiency and risk: Companies aim to maximize profits, so those that only focus on short-term rather than long-term goals may overlook the long-term consequences, which are highly likely to result in significant losses. Larger ports mean higher economic costs per port. The higher the degree of technological dependence, the

more significant an impact any single system failure could have on the operation of the port. Overall, in order to solve this problem, our main research question is why profit-maximizing port operators adopt high levels of automation and what risks are involved.

III. Analytical Framework

This paper presents a clear, systematic analysis of the economic logic underlying port automation decisions from the standpoint of neoclassical firm economics, which starts with the standard assumption that firms are fully rational, profit-maximizing, and make production and investment decisions on the basis of cost minimization and efficiency enhancement. Hence, it naturally leads to an evaluation of the efficiency gains and risks of port automation, followed by cogent policy recommendations.

a. Key Concepts

Technical Economies of Scale

When an enterprise expands its production scale, if it can produce goods or services more efficiently, technological economies of scale will occur. Factors such as labor specialization, more efficient utilization of machinery and equipment, and improvement of production processes may all lead to technological economies of scale. In neoclassical cost theory, average total cost is defined as the sum of average variable cost and average fixed cost:

$$ATC = AVC + AFC$$

Average variable cost is calculated as:

$$AVC = TVC / Q$$

In this study, firms reduce ATC by replacing manual labor with automated equipment, which increases efficiency and output (Q). In the short run, higher output lowers average variable cost, while in the long run, fixed costs are spread over a larger scale of operation, reducing average fixed cost. As a result, ATC declines, and the level of profit would increase even with a constant revenue, which enhances profitability and incentivizes port operators to expand automation.

Economic Cost

Economic cost refers to the total opportunity cost of all resources used in production, including both explicit costs (accounting costs) and implicit costs (the opportunity cost of self-owned resources that do not require direct monetary payment). The advancement in port automation can significantly reduce explicit labor costs and implicit costs due to higher efficiency, lower levels of energy waste, and fewer errors.

Because the estimation of implicit disruption costs is done using a port economic loss assessment model in this study, it is natural and logical to divide total downtime

losses into three well-defined components: direct losses, indirect losses, and ripple effects [15](Regional Studies in Marine Science, 2022).

$$E_{loss} = E_{direct} + E_{indirect} + E_{ripple}$$

Direct losses are computed as the product of the port's daily revenue and the number of outage days, while indirect losses stem from supply chain disruptions.

$$E_{indirect} \approx \sum(volume \times delay \times cost\ per\ unit\ delay)$$

Ripple effects are the general effects on upstream and downstream industries, and therefore can quite naturally be analyzed with economic models like the Input-Output model.

b. Logic of Application

This study conducts a case analysis from the perspective of neoclassical firm economics, combined with the concept of economies of scale, at three levels. First, it uses the economies of scale theory to explain the driving forces behind DP World's promotion of automation. Second, it applies the concepts of accounting cost and economic cost to analyze potential decision-making bias in firms. Third, it examines the relationship between economies of scale and operational risk. Based on this three-level analysis, the study proposes government and policy recommendations to address the potential issues arising from port automation.

IV. Case Analysis: The Motive Behind Actions, The Impacts Behind Cases

DP World (Dubai Ports World), one of Australia's largest container terminals and supply chain operators, is an example of a private firm. Also, it transferred to full private ownership in 2020 [12](CNBC, 2020) and has ports operating in numerous regions around the world. From the standpoint of neoclassical economic theory, the firm is assumed to seek profit maximization by minimizing costs and improving efficiency, which is precisely why DP World has publicly declared its commitment to using IT and technological innovation to boost processing efficiency and service quality [13](DP World, 2023). However, the company subsequently suffered a major cyberattack that disrupted operations at several Australian ports [10](Security Week, 2023). Other important actors in this setting are port users, namely shipping and trading firms, which depend on reliable, predictable port services, and the government, which has a limited but significant supervisory role in port security and national supply chain stability. According to authoritative reports and materials, namely positive analysis, we will present some normative evaluations regarding the logic, purpose, effectiveness, and outcomes of this company's efforts to enhance automation.

Because IT systems and autonomous technologies have greatly improved DP World's operational efficiency, DP World has joined forces with the German firm

SMS to develop the BOXBAY system, as a result of which energy consumption was reduced by 29% and container handling efficiency increased by 31%. DP World achieves 8 moves per hour [13](DP World, 2021) and has systematically tested autonomous vehicles to enhance internal transport efficiency [8](Newsdesk, 2026). From an economic standpoint, it is clear that although the initial investment costs are high, the technologies increase output over time, thereby lowering the average cost per unit and facilitating long-term profit growth. As profits grow due to the high efficiency of the operation process, DP World has deliberately expanded its global operations to strengthen its technological economies of scale, which is why it has become one of the world's leading port operators [4](Global Port Giants, 2025). With the effect of further economies of scale, there might be a shrinkage of their average total cost, which is favoured by autonomous systems' higher running efficiency. By using specialized machinery and robotics, the operation time is decreased substantially, which may help DP World to increase working efficiency and occupy a higher market share.

By achieving economies of scale to reduce average costs, this might be one of the strategies adopted by these private enterprises. From another perspective, we believe that reducing the total economic cost of enterprises in the long run is also reasonable and reliable. High port automation can bring operational improvements because it can lower overall economic expenditures by minimizing explicit and implicit costs [11](Schleich J, 2016). The reduction in explicit costs is attributed to automated processing equipment, which reduces labor and training costs. Coupled with digital tools like the BOXBAY automation system, it can minimize time and energy consumption to the greatest extent. For implicit costs, we believe that automation can reduce errors, delays, and underutilized capacity in manual operations, which is also one of the reasons why enterprises apply artificial intelligence to their production processes. Based on artificial intelligence coordination, it can improve processing efficiency, shorten turnaround time, and reduce opportunity costs due to idle capacity or business losses. In summary, automation can optimize resource utilization, significantly reduce economic costs, and enhance the economic advantages of ports.

A high degree of automation inevitably brings major risks: heavy reliance on AI and digital systems increases technological dependence and therefore exposes ports to greater cybersecurity threats. In highly automated operations, a system failure or cyberattack can stop critical processes that manual labor cannot easily replace, hence magnifying economic losses. Thus, we point out a problem: efficiency-driven automation creates risks alongside the increase in the company's profits. DP World reportedly uses AI in 98% of its supply chain operations [2](Ashcroft, 2024), which also explains the scale of losses during the recent cyberattack. Fortunately, the model for calculating the economic loss of ports is well established: direct losses can be reasonably estimated by multiplying daily revenue by outage days [15](Regional

Studies in Marine Science, 2022). According to the report, the annual revenue of the Australian port of Dubai Global Port is 976,239,000 US dollars. Converted to daily revenue, it is 976,239,000 US dollars / 365 ≈ 2,674,627.40 US dollars [6](IBIS, 2024). These ports were out of operation for three days, and they handled 40% of Australia's total freight volume [5] (ABC News, 2023). Therefore, the direct loss is calculated as 3 × 2,674,627.40 US dollars × 40% ≈ 3.2 million US dollars. Indirect losses can be reliably calculated from an average delay cost of $200 per container and a backlog of 30,000 containers, yielding indirect losses of roughly $18 million [1][5] (FreightAmigo, 2016; ABC News, 2023). Therefore, the total estimated loss is $21.2 million.

But perhaps more importantly, the incident caused significant non-monetary losses in terms of social impact. As reported in [3](Bermudez K 2023), in the three days after the cyber attack, nearly 30,000 shipping containers loaded with consumer goods were stranded at four major ports in Sydney, Melbourne, Brisbane, and Fremantle, leading to an economic loss of many millions of US dollars.

V. Implication and Proposal

Dividing the targeted proposal into two dimensions, which are the institutional level and the national level, respectively. We believe that our proposals could offer DP World an alternative way of operating, which could reduce the negative impacts brought by port automation effectively. In terms of the institutional level, DP World is confronted with the core issue of 98% of its supply chain relying on AI with no human backup[2] (Ashcroft, 2024). Therefore, establishing a comprehensive system is necessary in order to ensure safety. More specifically, the port could use human resources to replace the machinery when the system is shut down. When the port operators make their automation investments, they must retain the mechanism of increasing human involvement and maintaining the combination of AI and human labor. The specific standards include three dimensions.

First, the automation system should be divided into core functional modules that mainly focus on scheduling and loading, equipped with manual emergency operation plans, such as manual backup, and non-core functional modules [9](ITF, 2021). Second, they need to make security investment decisions through the Gordon–Loeb model instead of setting a fixed ratio. The Gordon-Lobb model provides a theoretical benchmark, indicating that the returns on securities investment will gradually decrease, but it is not the exact optimal value. We use this theory as an illustrative bond to assist our analysis there. This model shows that firms' investment in security shouldn't exceed 37% of the expected loss, because overinvestment will lead to diminishing marginal returns.

Meanwhile, DP World's heavy reliance on AI amplified the potential loss from system failures. Based on the calculations from the model used in the case analysis, DP World incurred an economic loss of $21.2 million due to the cyberattack, and the

reasonable upper limit for security investment is 37% of this loss. Calculations show that the optimal security investment should be 0.37 × 21.2 = $7.8 million. However, reports indicate that DP World's actual investment in cybersecurity reached $90 million [14](DP World, 2025), which is far in excess of the reasonable range. In this case, the excess investment in security may lead to cost waste; therefore, the institutions need to abandon sunk costs when encountering automation problems, as they shouldn't only consider profits but also take into account the security of overseas trade.

Intervention at the national level is necessary because enterprises' security investment may deviate from the socially optimal level that the Gordon–Loeb model suggests due to information asymmetry and other factors. Joint efforts by authorities and cybersecurity departments are necessary to implement tiered port automation supervision. For highly automated ports like DP World, they're required to disclose the proportion of sunk costs in automation investments quarterly, which can force enterprises to weigh sunk cost recovery against operational risks. They're also required to conduct reporting and risk assessment before major system upgrades.

However, these proposals also face feasibility challenges. The first is cost pressure: Global operators like DP World will need to allocate a specific percentage of automation budgets to security, while small ports face initial costs for connecting to the emergency platform. Therefore, both raise short-term operational expenses. The second is the difficulty with technology adaptation. The compatibility between the automated systems of some old ports and the manual emergency plans is poor, which might lead to short-term operational disruptions. The core trade-offs are equally notable. First is the balance between efficiency and risk. Mandatory increases in safety-related designs may lead to efficiency losses in the automated systems, but in the long run, this can improve supply chain stability by reducing the incidence of risk events. Second is the balance between regulation and innovation: detailed regulation may slow down the iteration of port automation technology, but it can also trade off the short-term slowdown in innovation speed for long-term operational safety.

VI. Research Limitations and Conclusion

Under the assumption of maximizing profits, private ports overly emphasize reducing explicit costs and promote economies of scale brought by automation, but underestimate the implicit costs and related risks. Through the analysis of the DP World case, it's obvious that it was driven by profit to promote automation, and ultimately suffered losses in a cyberattack. The proposals we've raised at the institutional and national levels can effectively balance the efficiency of automation and operational risks.

This analysis has certain limitations. Firstly, our framework cannot be applied to all

types of ports because we only use the private type of ports as the analytic target. Indeed, there are great differences between "government-led ports" and "private ports": for instance, government-led ports like Shanghai Yangshan Port can cover the costs used for guaranteeing safety through subsidies, while private enterprises like DP World are more likely to fail to implement regulations due to cost pressures. So ports owned by the public or partially owned by the government may result in different operational outcomes due to more comprehensive supervision and government control.

Secondly, this analysis doesn't take into account the differences in regional economic development levels. Some developing countries' ports may be unable to effectively implement certain requirements due to insufficient technology. Therefore, for different countries with varying levels of technological development, we cannot apply our theories to analyze whether automation brings harm or benefits to these countries, or to analyze what level of automation is effective and reasonable.

References

[1] AI logistics, insurance & trade finance platform | FreightAmigo. (2016). Retrieved from FreightAmigo website: https://www.freightamigo.com/en/

[2] Ashcroft, S. (2024, January 23). DP World Report: AI Vital in 98% of Supply Chain ops. Retrieved from supplychaindigital.com website: https://supplychaindigital.com/operations/dp-world-report-ai-vital-in-98-of-supply-chain-ops

[3] Bermudez, K. (2023, November 27). Government-Industry Collaboration Minimized Damages Following Hack of Australian Ports. Retrieved from FDD website: https://www.fdd.org/analysis/2023/11/27/government-industry-collaboration-minimized-damages-following-hack-of-australian-ports/

[4] Global Port Giants: Who Leads the Industry? (2025, March 12). Retrieved from Sinay website: https://sinay.ai/en/top-10-biggest-port-operators-in-the-world/

[5] https://www.abc.net.au/news/andi-yu/101931434. (2023, November 11). Australian ports shut down over cyber security incident impacting goods moving into and out of the country. Retrieved February 3, 2026, from Abc.net.au website

[6] IBISWorld. (2024). DP World Australia (Holding) Pty Ltd - Company Profile. Retrieved February 3, 2026, from Ibisworld.com website: https://www.ibisworld.com/australia/company/dp-world-australia-holding-pty-ltd/13120/

[7] Keen, S., & Standish, R. (2006). Profit maximization, industry structure, and competition: A critique of neoclassical theory. Physica A: Statistical Mechanics and Its Applications, 370(1), 81–85. https://doi.org/10.1016/j.physa.2006.04.032

[8] Newsdesk. (2026, January 23). DP World tests autonomous vehicles in live traffic at Antwerp Gateway, probing the future of terminal operations. Retrieved January 29, 2026, from Breakbulk.news website: https://breakbulk.news/dp-world-tests-autonomous-vehicles-in-live-traffic-at-antwerp-gateway-probing-the-future-of-terminal-operations/

[9] Ronan. (2021, April). ITF Transport Outlook 2021. Retrieved from ITF website: https://www.itf-oecd.org/itf-transport-outlook-2021

[10] Townsend, K. (2023, February 13). SecurityWeek Cyber Insights 2023 Series. Retrieved June 16, 2026, from SecurityWeek website: https://www.securityweek.com/securityweek-cybersecurity-insights-2023-topics/

[11] Schleich, J., Gassmann, X., Faure, C., & Meissner, T. (2016). Making the implicit explicit: A look inside the implicit discount rate. Energy Policy, 97, 321–331. https://doi.org/10.1016/j.enpol.2016.07.044

[12] Turak, N. (2020, February 17). Dubai's massive port operator DP World is delisting and returning to private ownership. Retrieved from CNBC website: https://www.cnbc.com/2020/02/17/dubais-dp-world-is-delisting-and-returning-to-private-ownership.html

[13] World, D. (2021, August 17). Successful real-world trial of BOXBAY high bay storage system completed. Retrieved from Successful real-world trial of BOXBAY high bay storage system completed website: https://www.dpworld.com/en/news/successful-real-world-trial-of-boxbay-high-bay-storage-system-completed

[14] World, D. (2025, December 17). DP World Invests Over US$90 Million in Port Security in the Dominican Republic. Retrieved February 3, 2026, from GlobeNewswire News Room website: https://www.globenewswire.com/news-release/2025/12/17/3207078/0/en/DP-World-Invests-Over-US-90-Million-in-Port-Security-in-the-Dominican-Republic.html

[15] Zhou, X., Dai, L., Jing, D., Hu, H., & Wang, Y. (2022). Estimating the economic loss of a seaport due to the impact of COVID-19. Regional Studies in Marine Science, 52(17), 102258. https://doi.org/10.1016/j.rsma.2022.102258