Proceedings of ICMRED 2026 Symposium: Financial Innovation, Risk Governance, and the Dynamics of Global Capital Flows
DOI: 10.54254/2754-1169/2026.BL34553

Mechanism of Risk Regeneration in High-Risk Industries Under Digital Supervision: Evidence from 13 Fireworks Enterprises

Jingyi Zhang

School of Management, Guizhou University, Guiyang, China
mc.jyzhang24@gzu.edu.cn

Abstract. Digital technology is widely seen as a key tool to enhance supply chain transparency and prevent accidents. However, findings indicate that technical compliance alone fails to reduce safety accident risks. This study attributes the paradox to deep institutional logic conflicts from forced digital supervision embedding. Safety-first regulatory logic conflicts with market-efficiency logic in high-risk industries, shifting physical operational risks to digital risks. This paper selects 13 cases of risk regeneration of fireworks and firecracker enterprises that have introduced digital supervision in the past three years, and uses grounded theoretical methods to explore how the fracture of institutional logic changes the trend of risk in the context of forced embedding of digital supervision, which eventually leads to the re-emergence of risk in another form. It is expected to provide a new theoretical perspective for understanding the paradox of digital governance in high-risk industries and practical enlightenment for designing more compatible intelligent regulatory policies.

Keywords: digital regulation, high-risk industries, risk management

1. Introduction

Today, digital supervision is widely applied in the safety governance of high-risk industries to enhance supply chain transparency and accident prevention [1]. However, the frequency of safety accidents has not been reduced significantly, and risks have emerged in more concealed forms. This study argues that the root cause lies not in digital technology itself, but in the institutional logic conflict caused by mandatory digital supervision, namely the clash between safety-first regulatory logic and market-efficiency logic in high-risk industries [2]. Such logic rupture drives supply chain participants to adopt strategic adaptive behaviors, which transform original physical operational risks into data authenticity risks and system vulnerability risks, making risks harder to identify and manage [3]. Supply chain risk management aims to identify, assess, mitigate and monitor supply chain risks that may cause disruptions, including operational, environmental and geopolitical risks [4]. The fireworks and firecracker industry, a typical high-risk, flammable and explosive sector, faces inherent safety risks across its entire value chain, complex distribution networks and volatile seasonal demand, making it an ideal context for studying risk evolution under digital supervision.

DOI: 10.54254/2754-1169/2026.BL34553

Most existing studies affirm the value of digital technology as a neutral tool, and abductive reasoning can comprehensively identify and evaluate digital technology applications in supply chain management [5]. A framework can be built based on digital transformation literature to summarize its benefits, challenges, key success factors and related technologies [6]. Meanwhile, some scholars have shifted their focus to institutional logic and structural tension in digital technology-enabled governance. Studies have constructed technology-system-social analysis frameworks from the perspective of technology sociology [7]. Analyzed the configuration of state, market and corporate logics in digital government cooperation via multi-period qualitative comparative analysis [8]. Other scholars explore how digital technology drives sustainable supply chain management, such as digital twin technology's role in green logistics [9]. The mediating role of supply chain mapping between DSCM and supply chain sustainability [10].

This study selects 13 cases of risk regeneration in fireworks enterprises with digital supervision in the past three years, and adopts grounded theory to construct a conceptual model of risk transformation. It aims to reveal how institutional logic fracture reshapes risk evolution through supply chain participants' strategic behaviors under forced digital supervision embedding. Theoretically, this study enriches institutional logic theory in risk management, proposes a new perspective for digital-era risk evolution and deepens the understanding of high-risk supply chain management. Practically, it provides a new theoretical perspective for understanding the digital governance paradox in high-risk industries and practical implications for designing compatible intelligent regulatory policies.

2. Study design and methodology

This study adopts grounded theory, collecting first-hand data from four representative fireworks enterprises via interviews and second-hand data from public digital supervision cases and documents. As seen in Table 1, following typicality and focus principles for grounded theory sampling, 13 cases are selected from integrated data, with 10 for grounded analysis and 3 for saturation testing.

Table 1. Case selection

	Region	Case type	Data sources	Sample usage
1	Liling City, Hunan Province	Illegal production during shutdown	Firsthand	Grounded research
2	Qingdao, Shandong Province	Purchase through informal channels to reduce the additional cost of Digitalization.	Firsthand	Grounded research
3	Anshun City, Guizhou Province	Illegal storage in abandoned rooms	Firsthand	Grounded research
4	Harbin, Heilongjiang Province	Cross-provincial online sales	Firsthand	Saturation analysis
5	Zhangzhou City, Fujian Province	Discrepancy between the account and reality	Secondhand	Grounded research
6	Bengbu City, Anhui Province	Abnormal flow identification code	Secondhand	Saturation analysis
7	Changsha City, Hunan Province	1054 fireworks transformation express packages	Secondhand	Grounded research

DOI: 10.54254/2754-1169/2026.BL34553

Table 1. (continued)

8	Xinyu City, Jiangxi Province	A fireworks store in Wanzai illegally transported 142 pieces	Secondhand	Grounded research
9	Changsha City, Hunan Province	Manufacturing and selling counterfeit thousands of miles of rivers and mountains fireworks	Secondhand	Grounded research
10	Beihai City, Guangxi Zhuang Autonomous Region	Safety training institutions lose surveillance video	Secondhand	Saturation analysis
11	Jinan City, Shandong Province	Selling fireworks while eating hot pot.	Secondhand	Grounded research
12	Changsha City, Hunan Province	Express delivery in violation of regulations and network receipt transportation	Secondhand	Grounded research
13	Hunan Province	A false evaluation report was issued by a safety evaluation agency	Secondhand	Grounded research

In the process of open coding, first of all, by dismantling the information in the case data, the semantics related to risk evolution are labeled as concepts. Then use unified standards to classify labels, refine and summarize labels in the same category, form related concepts, and constitute the main category. Finally, further analysis and abstraction of related concepts are carried out to concentrate and refine subcategories. The open coding process resulted in 103 tags and 34 concepts. The spindles are encoded along two coding paths: The first type of path further clusters open coding along the resulting subcategories, correlates independent categories, and combines two or more subcategories into a main category. The second kind of path refers to the conceptual dimension and analytical framework of existing research results, and tries to discover and construct the logical relationship between categories. Based on the above two paths, a total of 20 subcategories and 9 main categories are summarized in the existing subcategories at this stage, and the coding results are shown in Table 2.

Table 2. Main shaft coding result

Core category	Main category	Subcategory
A Avoiding regulatory logic	A1 Production process disconnection	A1-1 Illegal production during shutdown A1-2 Production beyond the licensed scope A1-3 Evading the electronic waybill system
	A2 Concealment of storage links	A2-1 Illegal storage of abandoned rooms A2-2 Illegal storage in residential areas A2-3 Off account warehouse
	A3 Non-standardization of transportation	A3-1 Illegal express delivery A3-2 Vehicle transportation of non-hazardous chemicals A3-3 Network platform private order
B Cost transfer logic	B1 Procurement channel sinking	B1-1 Purchase through informal channels B1-2 Cross-provincial network procurement of unqualified products B1-3 Bypass wholesaler direct purchase

DOI: 10.54254/2754-1169/2026.BL34553

Table 2. (continued)

	B2 Sales model variation	B2-1 Illegal sales of webcast B2-2 Direct selling across provinces, bypassing regulatory areas B2-3 Community hidden bill
C Payable compliance logic	C1 Flow direction information distortion	C1-1 Discrepancy between account and reality C1-2 Abnormal flow direction identification code C1-3 Separation of electronic account and physical object
	C2 Monitoring data failure	C2-1 Training surveillance video lost C2-2 Tampering with transport GPS tracks C2-3 Misrepresentation of inventory data
D Responsibility drift logic	D1 Third-party evaluation distortion	D1-1 False report of a safety assessment organization D1-2 Illegal release by the testing agency
	D2 Regulatory Commission failure	D2-1 Data omission of the digital supervision platform D2-2 Going through the motions in government purchasing services

Selective coding further excavates the core categories by continuing to analyze the connotative nature of the main categories. By further analyzing the relationship between the core category and other categories, the logical framework of risk regeneration of high-risk industries caused by digital supervision is presented. To a certain extent, the cases of fireworks and firecracker enterprises reflect the logical chain of institutional logical conflict, strategic adaptation, and risk form transformation. The conceptual model of risk evolution logic of high-risk industries constructed in this paper is shown in Figure 1. Nine main categories are classified into four core categories: regulatory evasion logic, cost transfer logic, data compromise logic and responsibility drift logic, Around the core category, the whole process of risk regeneration of high-risk industries caused by digital supervision can be summarized as the logical fracture of safety and efficiency caused by the forced embedding of digital supervision, which drives the main body of the supply chain to adopt four strategic adaptation behaviors of evasion, transfer, compromise and drift, resulting in the transformation of the original physical operation risk into the regeneration risk of digital form, forming a governance paradox of continuous risk regeneration under the appearance of compliance.

This paper selects three cases for saturation analysis, and encodes the three-case data to verify the internal relationship structure of various categories in the process of risk transformation. After testing, the three case materials all conform to the logical chain of institutional logical conflict strategic adaptation risk form transformation, and no new concepts or categories are found in the coding process, indicating that the main and sub-categories of this paper and their internal relationship structure are stable, and the coding results have approached saturation.

DOI: 10.54254/2754-1169/2026.BL34553

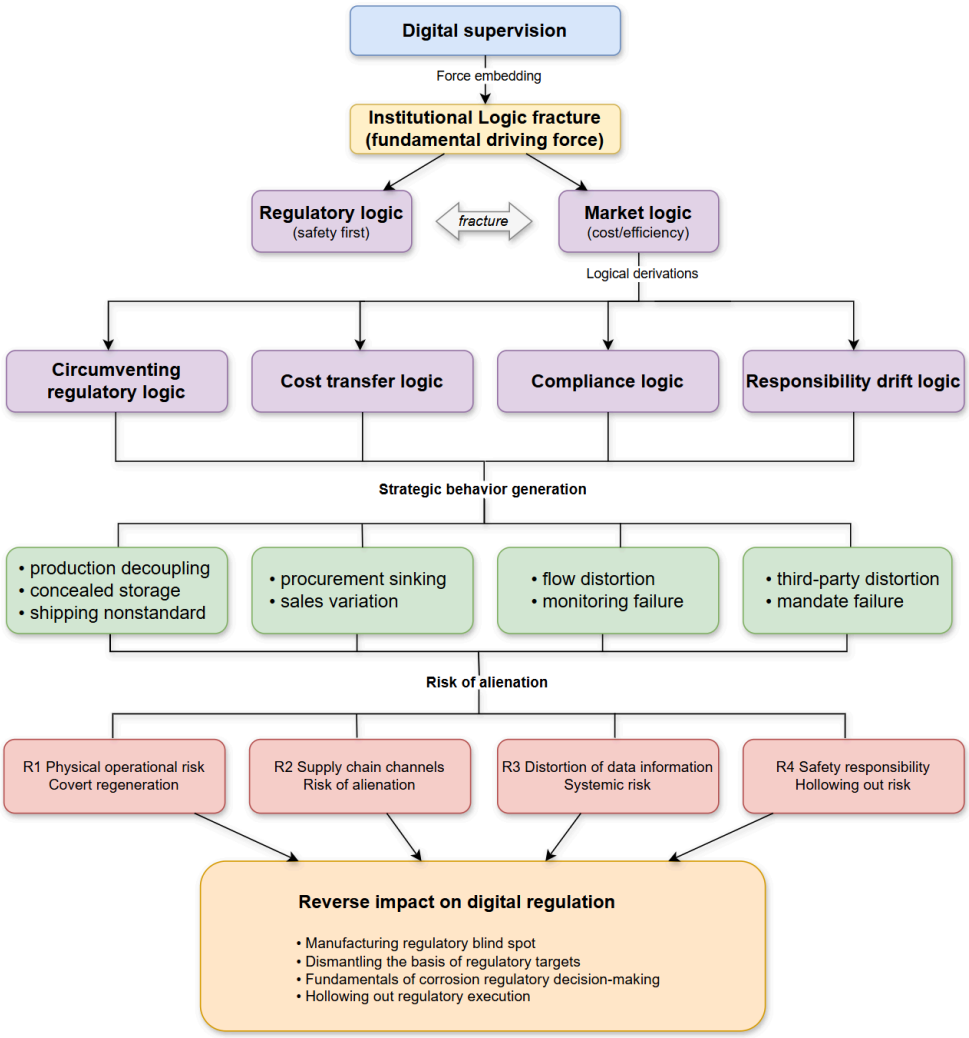

Figure 1. Risk evolution chart of high-risk industries (picture credit: original)

3. Analysis and discovery

Based on the aforementioned grounded theoretical results and the conceptual model of institutional logical conflict strategic adaptation risk from transformation, this paper analyzes the risk evolution mechanism of the fireworks industry under the compulsory embedding of digital supervision. The rupture of regulatory logic and market efficiency logic does not directly produce accidents, but drives the generation of strategic behavior by deriving four organizational behavior logics as intermediary mechanisms, thus realizing the transfer and regeneration of risk forms. Under the high pressure of digital supervision, there is a sharp friction between the regulatory logic of safety first and the market logic of cost efficiency first. In order to survive in this gap, the main body of each node in the supply chain has developed four representative types of subsidiary behavior logic. Such behaviors represent direct resistance to regulatory logic.

The study finds that supply chain actors do not abandon violations but shift physical operations to digital monitoring blind spots via decoupling, concealment and non-standard strategies, such as illegal production during shutdowns, storage in abandoned buildings and transport by ordinary express delivery. This logic creates regulatory coverage vacuums that exclude explosion and leakage

DOI: 10.54254/2754-1169/2026.BL34553

risks from digital system warnings. The cost transfer logic arises from rising digital compliance costs (hardware, identification codes, special logistics) and market efficiency-driven demand for lower prices, manifesting as sunk procurement channels and varied sales models. Such behaviors shift compliance costs to public security and replace formal digital tracking with informal circulation networks. The coping compliance logic represents symbolic compliance by firms unwilling to bear full compliance costs, involving data fraud like inconsistent accounts, tampered GPS tracks and lost training videos, which triggers data trust crises and separates physical flows from information flows. The responsibility drift logic emerges as third-party agencies collude with enterprises or perform duties perfunctorily, diluting safety responsibilities and weakening governmental supervision.

Based on the above four behavioral logic paths, this paper finds that the risk nature of high-risk industries has changed fundamentally. The transfer of risk sources has shifted from the original physical factors, such as equipment failure, personnel operation error, and natural conditions, to the human technology mixed factors, such as data entry distortion, system algorithm blind area, and network security vulnerabilities. The concealment of risk performance is enhanced, physical explosions have clear acoustic and optical smoke signals, while data fraud and monitoring failure are silent. Regulators are no longer dealing with outright illegal production, but with phantom security woven by perfect data. Finally, due to the long-term deviation between information flow and physical flow, once an emergency occurs, the digital emergency command system will make wrong decisions by relying on wrong data, resulting in the cumulative amplification of risks under the cover of the digital system, and may eventually break out as more severe physical accidents.

4. Revelations and suggestions

Based on the findings, policy suggestions include reconstructing data quality control priorities, integrating corporate culture with operational processes, strengthening third-party joint liability, building digital supply chain buffers and optimizing technology system design. The attention of regulatory authorities should shift from simply uploading data to checking data quality. It is suggested to develop cross-modal data verification algorithms, such as comparing meter data with production data and video behavior analysis, accurately identifying compliance behavior, and cracking down on digital games with inconsistent accounts and facts.

For enterprises, it is emphasized that when implementing digital traceability, enterprises should go beyond the compliance level and truly integrate it into the safety culture and operation process of enterprises in order to achieve effective risk management. To establish a comprehensive safety concept, enterprises should regard digital traceability as an opportunity to improve the overall safety management level. Integrate the safety concept into the corporate culture to ensure the safety of the whole production and operation process. Strengthen staff training and improve their data entry and management capabilities. Actively identify new risks, recognize various risks that may be brought about by digital traceability, and actively take measures to identify, assess, and manage them. In view of the logic of responsibility drift, it is necessary to establish a lifelong traceability mechanism for safety evaluation and test results. If the accident exposes that the evaluation report is seriously inconsistent with the actual situation on site, the cost of violations by third-party institutions and signatories should be greatly increased to prevent collusion and failure in regulatory entrustment. Recognize the Survival Logic of small and micro entities in high-risk industries. While promoting the digitalization of the whole chain, necessary and low-cost physical emergency channels should be retained to avoid forcing enterprises to completely escape the regulatory system due to excessive cost pressure.

DOI: 10.54254/2754-1169/2026.BL34553

For technology providers, when designing digital traceability systems, full consideration should be given to user behavior, institutional environment, and potential sociotechnical risks. Design a user-friendly and easy-to-operate digital traceability system to reduce the compliance cost and operation difficulty of enterprises. In the system design, data security and privacy protection are fully considered, and advanced encryption technology and authority management mechanisms are adopted to prevent data leakage and abuse. Customized according to the specific needs of different industries and enterprises, and upgraded with the development of technology and the change of regulatory requirements. Risk assessment and early warning functions are integrated into the system to help enterprises and regulators find potential risks in time.

5. Conclusion

Thirteen risk regeneration cases of fireworks enterprises under digital supervision illustrate the risk evolution paradox in high-risk industries' digital transformation. This paper believes that the rupture of Institutional Logic caused by the forced embedding of digital supervision is the deep driving force of risk evolution. The fundamental conflict between regulatory logic and market efficiency logic makes digital technology from an enabling tool to a logical game field. Under the pressure of logical fracture, the main body of the supply chain has developed four derivative logics, namely, avoiding supervision, cost transfer, coping with compliance and responsibility drift, and has taken corresponding strategic actions. These behaviors are a bridge between macro institutional conflicts and changes in micro risk patterns. Digital supervision does not eliminate risks, but promotes the structural transformation of risks. The original physical operation risk has been partially transformed into a more hidden and systematic digital regeneration risk, which leads to the dilemma of good data and difficult hidden dangers in safety management.

This paper enriches the explanatory power of Institutional Logic Theory in the field of risk management. Previous studies have focused on the enabling role of technology itself. This paper proves that the actual effectiveness of technology depends on the institutional soil it is embedded in. When the technical logic is forcibly replaced rather than compatible with the original organizational logic, it will lead to unexpected risk variation. In addition, this paper proposes the transformation path from physical risk to data risk, which provides a new analytical framework for understanding the digital paradox. Limitations include insufficient breadth and depth of data collection owing to constrained research resources. Based on the limitations of this paper, future research can explore how digital traceability interacts with local institutional logic and affects risk dynamics in fireworks supply chains in different countries and regions. The differences of different digital technologies in risk translation are compared, and the unique roles of different digital technologies, such as blockchain, Internet of Things, and big data in risk translation and reproduction are compared. A multi-agent game and complex system modeling, a game theory model is constructed, and multiple participants and detailed strategic choices are included to more comprehensively simulate and analyze the risk reproduction mechanism in the supply chain of high-risk industries.

References

[1] Xun, W., Du, X., Li, M. et al. (2025) Technology-Enabled Traceability and Sustainable Governance: An Evolutionary Game Perspective on Multi-Stakeholder Collaboration. Sustainability, 17(23), 10855-10855.
[2] Herold, D.M. and Marzantowicz, Ł. (2023) Supply Chain Responses to Global Disruptions and Its Ripple Effects: An Institutional Complexity Perspective. Operations Management Research, 16(4), 2213-2224.
[3] Tang, C.S. (2006) Perspectives in Supply Chain Risk Management. International Journal of Production Economics, 103(2), 451-488.

DOI: 10.54254/2754-1169/2026.BL34553

[4] Chopra, S. and Sodhi, M.S. (2014) Supply Chain Risk Management: What Are the Challenges? Supply Chain Management Review, 18(4), 22-29.
[5] Kim, H.S. (2025) A Review of Supply Chain Digitalization and Emerging Research Paradigms. Logistics, 9(2), 47.
[6] Isaias, B., António, G., Nursultan, S. et al. (2024) Towards the Path of Process Digitalization: A Systematic Literature Review. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 15(1), 1-27.
[7] Chen, G. and Zheng, L. (2026) The Institutional Logic of Digital Technology Enabling Grassroots Emergency Management — Based on the Analysis of Technological Sociology. Journal of Henan Normal University (Philosophy and Social Sciences Edition), 53(2), 33-41.
[8] Gong, Y. and Yang, Y. (2025) Analyzing Digital Government Partnerships: An Institutional Logics Perspective. Government Information Quarterly, 42(1), 101987-101987.
[9] Liu, Z. (2025) Research on the Role of Digital Twin Technology in Green Logistics and Sustainable Supply Chain Management. Integration of Industry and Education Journal, 4(4), 58-68.
[10] Mubarik, S.M., Khan, A.S., Gunasekaran, A. et al. (2025) Unlocking the Potential of Digital Technologies for Sustainable Supply Chain Management Strategies. Supply Chain Forum: An International Journal, 26(3), 358-378.