The AI-Driven Resilience Engine: Research on the Framework Construction and Behavioral Logic of BCM Agents

Wulong Gao[1] Jinqin Guo[2]

(1.Shenzhen Aisi Technology Co., Ltd., 2705, Wensheng Center, Wenjin Plaza, No.23 , Luohu District, 518020, Shenzhen City, Guangdong Province, China.

2 Taiyuan Institute of Technology, No. 31 Xinlan Road, Jiancaoping District, 030008, Taiyuan City, Shanxi Province, China)

ABSTRACT With the deepening of digital transformation, the business environment and cybersecurity threats faced by enterprises are becoming increasingly complex and volatile. Traditional Business Continuity Management (BCM) models, which rely heavily on manual labor and passive response, can no longer meet organizations' urgent demand for "resilience." The explosion of Generative Artificial Intelligence (GenAI) and Agent technologies provides a novel paradigm for the intelligent and automated reconstruction of BCM. This paper takes the "BCM Agent Framework and Behavioral Logic Diagram" as its research object, systematically deconstructing its core closed-loop logic of "Continuous Perception, Generating Recommendations, Guiding Actions, Validating Capabilities, and Promoting Growth." Firstly, the paper analyzes the pain points of digital transformation currently facing BCM. Secondly, it deeply dissects the seven-layer architecture system of the BCM Agent, focusing on the core engine's seven capability modules, the structured precipitation mechanism of the organizational memory base, and the seven-step closed-loop behavioral logic from perception to capability enhancement. Thirdly, combining the latest practical cases in the financial industry and intelligent operations, it demonstrates the core value of AI-BCM Agents in risk prediction, automated emergency response, and cross-departmental collaboration. Finally, drawing on research results from core journals in the past three years, this paper proposes future trends and governance challenges for BCM Agents, providing theoretical references and practical pathways for enterprises to build a "trustworthy, visible, and controllable" digital resilience system.

Keywords Business Continuity Management; Intelligent Agents; Digital Transformation; Generative AI; Resilience Governance; AIGC.

1.INTRODUCTION

In today's highly uncertain VUCA (Volatile, Uncertain, Complex, Ambiguous) era, Business Continuity Management (BCM) has leaped from being a "cost center" in enterprise operations to a "baseline project" guaranteeing survival and development. With the deep penetration of cloud computing, big data, and the Internet of Things, enterprise IT architectures and business processes have become unprecedentedly complex, and the interdependence of supply chains has intensified dramatically. Simultaneously, the frequent occurrence of ransomware attacks, geopolitical conflicts, and sudden public health events has led to business interruption risks exhibiting characteristics of high frequency, long tails, and compounding effects.

Traditional BCM systems rely heavily on human experience and periodic drills. This model suffers from significant lag and static limitations: risk identification often depends on regular paper-based or offline scanning, making it difficult to capture micro-level abnormal fluctuations in systems; the execution of emergency plans requires extensive cross-departmental manual coordination, resulting in low efficiency during golden recovery windows; more critically, traditional BCM lacks structured review and dynamic knowledge precipitation of historical events, causing enterprises to repeatedly "pay tuition fees" when facing similar risks.

In recent years, breakthrough progress in Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs), represented by ChatGPT, has brought dawn to solving these pain points. AI is no longer merely an auxiliary analysis tool but has evolved into a "digital employee" capable of autonomous perception, reasoning, planning, execution, and feedback. In this context, constructing a "BCM Agent" framework that integrates large model

capabilities to achieve a leap from "passive defense" to "active resilience" has become a focal point for both academia and industry. Based on the "BCM Agent Framework and Behavioral Logic Diagram," this paper aims to deeply analyze the operational mechanisms of AI-driven BCM and explore its practical application value in enhancing organizational digital resilience.

2 Deconstruction of the BCM Agent Framework and Core Logic Analysis

The BCM Agent is not a mere accumulation of algorithms but a complex adaptive system integrating perception, cognition, decision-making, and action. Its underlying architecture covers a complete technology stack from foundational support to top-level interaction, with its core logic reflected in the operation of the "Core Engine" and the iteration of "Organizational Memory."

2.1 Seven-Layer Architecture: A Panoramic View from Support to Interaction

The framework constructs seven tightly coupled layers from bottom to top:

Platform & Integration Layer (Support): As the foundation of the system, it is responsible for breaking down data silos. It achieves data integration through tools like ITSM (IT Service Management) and CMDB (Configuration Management Database); application integration through platforms like Teams and DingTalk; and ensures high availability through cloud/private deployment, guaranteeing the stable operation of agents in complex hybrid cloud environments.

Input Layer (Context & Input): Provides multi-dimensional information fuel. It includes not only static "Enterprise Context" (e.g., organizational structure, asset inventory, regulatory compliance requirements) but, more importantly, introduces "Dynamic Inputs" such as incident/exception information, daily operational data, and audit assessment results, providing the basis for real-time situational awareness.

User & Interaction Layer & Interaction Methods: Clarifies the system's service targets, covering management, BCM teams, business owners, and IT teams. In terms of interaction methods, it breaks through the limitations of traditional interfaces by introducing "Conversational Interaction (Natural Language)," "Workbenches/Dashboards (Visualization)," and "Tasks & Reminders (Proactive Push)," significantly lowering the barrier to entry for non-technical personnel using BCM tools.

BCM Agent (Core Engine) & Tools & Capabilities: The "Brain" of the system, responsible for complex logical processing (detailed below).

Organizational Memory (Memory): The "Experience Base" of the system, responsible for the structured precipitation of capability evidence.

Output Layer (Value & Results): Transforms the processing results of the agent into "Dashboards" visible to management, executable "Action Outputs," and implementable "Capability Development" plans.

2.2 Core Engine: Chain Collaboration and Intelligent Emergence of Seven Modules

The core engine consists of seven key modules connected in series, forming an assembly line for the agent to process complex BCM tasks:

Understanding & Perception: Utilizes NLP (Natural Language Processing) technology to parse unstructured text, understand organizational sentiment, identify key dependencies, and monitor changes and potential risk blind spots in the internal and external environment.

Knowledge & Skills: Relying on RAG (Retrieval-Augmented Generation) technology, it transforms the BCM knowledge system, industry best practices, and regulatory standards into the agent's "built-in brain," ensuring the compliance and professionalism of its recommendations.

Reasoning & Planning: Based on graph reasoning and rule engines, it conducts impact analysis on risks and deduces potential scenarios, formulating scientific task lists and plans for subsequent actions.

Generation & Guidance: Combining simulation/exercise engines, the agent can generate specific activities and plans, guidance suggestions, and automatically draft structured communication reports.

Collaboration & Execution: Assigns generated tasks to specific responsible persons, monitors progress, and provides decision support and escalation suggestions, bridging the gap between "strategy" and "execution."

Observation & Recording: Automatically captures behaviors and events, conducting structured Observation to ensure every emergency response is documented.

Evaluation & Learning: Evaluates capability scores, discovers patterns and trends, and continuously updates knowledge and models through root cause analysis, completing the system's self-evolution.

2.3 Organizational Memory: Structured Evidence Base and Knowledge Graph

Organizational Memory is the core feature distinguishing the agent from traditional software; it breaks the fragmentation of information. The framework designs five highly structured memory bases:

Activity Base & Task Base: Breaks down long-cycle BCM activities into standardized micro-task units, clarifying participating roles, responsibilities, and processes.

Observation Base & Scenario/Inject Base: Records every risk trigger (Trigger), impact (Impact), and response evidence (Evidence), while precipitating the background and objectives of various injection exercise scenarios.

Capability Base & Pattern Base: Quantifies the organization's current maturity level and key gaps, summarizing success patterns, anti-patterns, and behavioral patterns to provide a basis for analogy reasoning in future decisions.

3 Behavioral Logic Loop: A Seven-Step Advancement from Perception to Capability Enhancement

The greatest value of the BCM Agent lies not only in point-wise intelligence but also in its construction of a continuous closed loop of "Perception-Analysis-Action-Evolution." The bottom of the framework clearly depicts this seven-step behavioral logic:

Perceive & Identify: The system monitors changes and signals in real-time, identifies risk impacts, and outputs a "Risk/Issue List."

Analyze & Reason: Conducts deep analysis of risks, identifies capability gaps, and outputs "Analysis Results & Gaps."

Plan & Generate: Generates specific activities, drill plans, tasks, and steps based on the gaps, outputting "Plans/Tasks/Recommendations."

Execute & Collaborate: Drives task assignment and execution across departments and systems, outputting "Execution Records & Status."

Observe & Record: Marks decision points and issues throughout the process, outputting structured "Observations."

Evaluate & Insight: Assesses capability performance, discovers patterns and root causes, and forms an "Evaluation & Insight" report.

Improve & Grow: Translates insights into specific improvement plans and roadmaps, updates knowledge and models, and finally feeds back into the input layer, completing a full cycle of evolution.

This closed-loop mechanism ensures that the BCM system is not a static document set in stone but a "living system" that dynamically adjusts with business development and threat evolution.

4 Empirical Analysis: Cutting-Edge Application Scenarios of AI-BCM Agents

In recent years, many leading domestic and international enterprises have begun exploring and implementing the BCM Agent architecture, achieving remarkable results.

4.1 Financial Industry: KunLun Bank's AI-BCM Practice

KunLun Bank, relying on the KunLun Large Model and integrating AI middle-platform and knowledge graph technologies, has built a full-process intelligent system for supply chain risk monitoring and incident emergency response. By quantifying risks and providing forward-looking warnings, the project achieves the goal of "business continuity and zero data loss." The agent can crawl status data from supply chain nodes in real-time. When potential liquidity risks or external attacks are detected, it automatically triggers emergency plans and coordinates resource allocation across various business departments, effectively enhancing the risk resistance capability of financial services.

4.2 Intelligent O&M and Network Resilience: Bank of Communications' Network O&M Large Model

The Bank of Communications, in collaboration with Huawei, has created a new paradigm for network-intelligent O&M targeting duty handling and production change scenarios. Its constructed "Emergency Repair Agent" can automatically perform multi-dimensional fault data correlation analysis. Upon receiving alarm information, the agent extracts data from alarm platforms, change platforms, and network health data in parallel, performing root cause inference through the collaboration of large and small models. For instance, during a core transaction system latency event, the agent quickly ruled out network bandwidth bottlenecks, accurately pinpointed an impending Redis cluster memory overload issue, and automatically triggered elastic scaling suggestions, preventing a potential system downtime.

4.3 Enterprise-Level Automated Resilience Architecture: RealAgent's Fault-Tolerance Mechanism

As large models become deeply embedded within enterprises, the stability of the large model services themselves becomes a new risk to business continuity. Addressing issues like API timeouts or crashes in services like DeepSeek, the industry has proposed a resilient architecture based on "cloud redundancy + private deployment + RealAgent automated fallback." RealAgent possesses non-invasive automation capabilities and deep planning abilities. When cloud models fail, the agent can take over local business processes, achieving minute-level fault self-healing and cross-system data replenishment, reducing the Mean Time To Repair (MTTR) from hours to minutes.

5 Key Technologies and Frontier Dynamics

The construction of BCM Agents involves the intersection of multiple disciplines. The following three technological trends are particularly critical:

Deep Integration of RAG (Retrieval-Augmented Generation) and Knowledge Graphs: Pure generative AI is prone to "hallucinations." In the realm of BCM, where enterprise survival is at stake, accuracy is paramount. RAG technology allows agents to retrieve factual evidence from the enterprise's private, up-to-date knowledge base (e.g., emergency manuals) before generating recommendations. Combined with knowledge graphs modeling complex business dependencies, agents can perform more accurate causal reasoning.

Multi-Agent Systems (MAS): Facing complex emergencies, a single agent is often inadequate. The future trend is to build Multi-Agent Systems, establishing specialized "Risk Assessment Agents," "Resource Scheduling Agents," and "Communication Liaison Agents." These agents possess different areas of expertise and can solve comprehensive cross-departmental BCM challenges through negotiation and collaboration.

Large-Small Model Collaboration and Agentic Workflow: As demonstrated by the practice at the Bank of Communications, the industry is shifting from "Large Model Supremacy" to "Large-Small Model Collaboration." Large models handle complex semantic understanding and strategy generation, while lightweight small models or traditional machine learning algorithms handle high-concurrency

numerical calculations, log noise reduction, and pattern matching. This collaborative mechanism not only improves inference performance but also reduces computational costs.

6 Conclusion and Outlook

Based on the "BCM Agent Framework and Behavioral Logic Diagram," this paper systematically argues for the reconstructive value of AI technology in traditional business continuity management systems. By introducing the agent architecture, enterprises can build a resilient hub capable of continuous perception, autonomous reasoning, collaborative execution, and dynamic evolution.

Looking ahead, the development of BCM Agents will exhibit the following trends:

Shift towards "Resilience Governance" Paradigm: With the proliferation of GenAI, BCM Agents must not only address technical failures but also possess the ability to govern new types of risks such as algorithmic bias and data leakage. The focus of governance will shift from simply "assigning responsibility and hitting nodes" to building a resilient mechanism for institutional self-repair and continuous learning.

Strengthening Explainability in "Human-Agent Collaboration": In decisions involving major business interruptions, fully black-box AI struggles to gain management trust. Future BCM Agents must find a balance between "autonomous decision-making" and "human oversight," providing transparent, traceable, and explainable reasoning processes to enhance human confidence in judgment.

Full-Stack Localization and Security Control: As national requirements for data sovereignty increase, BCM Agents must be capable of running stably in localized hardware and software environments, ensuring that the enterprise's "last line of defense" remains firmly in its own hands under extreme circumstances.

In conclusion, the construction of BCM Agents is a systematic project. It requires not only cutting-edge AI technology empowerment but also synchronous transformations in management strategic consensus, cross-departmental process reshaping, and organizational culture. Only in this way can enterprises navigate steadily and far in the turbulent waves of the digital age.

REFERENCES

[1] The State Council of the People's Republic of China. The Belt and Road Initiative: Progress, Contribution and Outlook[R]. Beijing: Foreign Languages Press, 2019.
[2] Ministry of Digital Development, Communications and Mass Media of the Russian Federation. Strategy for the Development of the Digital Economy of the Russian Federation until 2035[R]. Moscow: Ministry of Digital Development of Russia, 2020.
[3] Li Y. Digital Empowerment and the Development of Cross-Border Language Services Under the Belt and Road Initiative[J]. Journal of International Communication, 2022(3): 45-58.
[4] Wang H, Ivanov S. Current Situation and Countermeasures of China-Russia Cross-Border Language Service Cooperation[J]. Russian Language and Literature Studies, 2023(2): 78-85.
[5] Zhang Q. The Construction of Intelligent Translation Platform for China-Russia Cross-Border Trade[J]. Journal of Border Economics and Administration, 2022(4): 92-100.
[6] Smith J. Digital Transformation of Language Service Industry in International Cooperation[M]. New York: Springer, 2021.
[7] Petrova M. Cross-Border Language Cooperation Between China and Russia in the Digital Era[J]. International Journal of Language and Communication Studies, 2022, 10(2): 34-47.
[8] Translators Association of China. Annual Report on the Development of the Language Service Industry in China (2023)[R]. Beijing: Translators Association of China, 2023.
[9] Huang L., & Kuznetsov A. Cross-border data governance in the digital silk road: A comparative study of China and Russia[J]. Digital Policy Studies, 2024, 5(1): 22-39.
[10] Zhao X. Interdisciplinary talent cultivation for digital language services: A case study of Sino-Russian cooperation[J]. Journal of Higher Education and Internationalization, 2023, 7(2): 105-118.