Data Governance Collaboration and Resilience Reference Architecture for Road Emergency Response

Haiyun Sun[1], Xueyan Bo[2,*], Dongdong Guo[3]
[1]Party School of the CPC Shandong Provincial Committee (Shandong Academy of Governance), Jinan, Shandong, China
[2]Disaster Reduction Center of Shandong Province, Jinan, Shandong, China
[3]Shandong High-Speed Airport Logistics Development Co., Ltd., Jinan, Shandong, China
**Corresponding Author*

Abstract: In the context of massive traffic volumes, extreme weather conditions, and cross-domain coordination, road emergencies often exhibit characteristics of "rapid onset, wide propagation, and high susceptibility to misinformation." Addressing these governance challenges, this study reconceptualizes holistic situational awareness-traditionally treated as a technological issue-into an integrated paradigm of governance, coordination, and resilience. To this end, it proposes a "Three-Layer–Two-Chain–Three-Flow" reference architecture for road emergency management. Methodologically, the study introduces templated implementations of the RACI matrix and DSC contract, specifying "who accesses which data fields, for what purpose, at what time, and with what traceability mechanisms." It further establishes a multi-tiered release, public communication, and navigation alignment mechanism to ensure consistency across information sources, interfaces, and interpretations. Leveraging zero-trust principles with minimal authorization and degradation–fault tolerance–recovery mechanisms for low-connectivity environments, the framework translates technical capabilities into actionable organizational authorizations and position-specific SOPs. Additionally, version governance-featuring semantic versioning, grayscale release, and rollback control-safeguards the semantic stability and traceability of rule evolution. Rather than relying on contrastive empirical validation, the proposed technical pathway offers an implementable, auditable, and transferable institutional model for provincial and municipal road networks and multi-agency emergency coordination, contributing to the development of resilient, adaptive, and accountable road governance systems.

Keywords: Roadway Emergency Response; Data Governance; Resilience Governance

1. Introduction

1.1 Background

In recent years, road transportation systems have increasingly operated under compounded pressures stemming from massive traffic volumes, extreme weather conditions, and the growing need for cross-domain coordination. Under these circumstances, road emergencies are occurring with greater frequency, spreading more rapidly, and exerting broader societal impacts. Consequently, emergency management has evolved from a model of intra-departmental response toward a paradigm of cross-departmental, cross-hierarchical, and cross-ecosystem collaborative governance. The proliferation of next-generation digital infrastructures-such as pervasive sensing networks, vehicle-road cooperative systems, cloud-edge collaboration frameworks, low-altitude platforms, and integrated navigation ecosystems-has substantially improved the accessibility of information during emergency response. However, information accessibility does not necessarily imply information usability, nor does usability guarantee that response plans are operationally executable. The critical governance challenge lies in what can be termed the "last mile": how to transform fragmented data distributed across diverse stakeholders and technical systems into authoritative, coherent communications and accountable, time-sensitive actions within the smallest possible decision window.

Against this backdrop, the concept of All-Domain Situational Awareness (All-Domain, SA) has expanded beyond its traditional technological connotation of data collection and fusion. It now represents a comprehensive governance proposition that spans three cognitive and operational layers-perception, comprehension, and projection-while embedding itself within the normative structures of rules, processes, responsibilities, and accountability [1]. In this sense, SA demands the unification of data flows, control flows, and policy flows across the four functional chains of information acquisition, decision-making, execution, and post-event review. This integration provides a measurable and auditable governance framework that enables both interdepartmental coordination and responsive social engagement.

Based on this conceptual grounding, this paper seeks to address three interrelated research questions:

(1) Architectural Integration. How can an integrated reference architecture be designed to reconcile cross-departmental data governance collaboration with resilience assurance, ensuring that the "information-decision-execution-review" process forms an auditable and adaptive feedback loop?

(2) Institutional Implementation. Under multi-stakeholder conditions, how can data-sharing contracts and RACI governance matrices institutionalize graded information release, minimal-necessity access, and purpose limitation?

(3) Operational Translation. How can technical degradation mechanisms (e.g., those developed for weak or disconnected networks) be translated into resilience governance clauses and position-specific SOPs, while aligning with version governance and iterative review to establish scalable policy pathways?

1.2 Research Framework

To address these questions, the study proposes an All-Domain Situational Awareness "Data Governance Collaboration and Resilience Reference Architecture" specifically designed for road emergency management. The architecture integrates technological capacities and institutional arrangements into a unified design framework structured around the principle of "Three-Layer+Two-Chain+Three-Flow." Specifically, the three layers-governance, coordination, and resilience-span two operational chains (perception-analysis-command-review), while the data, control, and policy flows function as first-order abstractions that guide interaction across components. Through the methods of contractualization, templating, and versioning, this framework ensures that cross-departmental collaboration is executable, measurable, and accountable.

The remainder of this paper is structured as follows. Section 2 reviews the literature and policy practices related to situational awareness technologies, data governance, and resilience governance, clarifying the study's theoretical foundation and identifying research gaps. Section 3 defines key concepts and constructs the analytical framework, elaborating on the core elements and interrelationships of the "Three-Layer+Two-Chain+Three-Flow" model. Section 4 presents the design of the data governance collaboration model and graded release mechanisms. Section 5 details the overall reference architecture for All-Domain SA in road emergency contexts. The final section proposes a policy design roadmap and concludes with implications for resilient and accountable governance in complex transportation systems.

1.3 Research Methodology

This study is grounded in a broader and more responsible innovation governance framework [2], adopting a three-stage methodological pathway of design-validation-normative formalization. It follows a design-oriented research (DOR) approach as its main methodological trajectory, complemented by a mixed paradigm that integrates institutional and policy analysis with contextualized validation. The research objective is not to report performance metrics from a single engineering experiment but to generate reusable, auditable, and transferable outputs-namely, a reference architecture, institutional templates, and an actionable implementation roadmap.

Additionally, the study seeks to advance the understanding of risk governance policies, aligning the foundational principles and objectives of innovation with broader socio-economic, environmental, health, and safety considerations [3]. This orientation embodies a responsible innovation ethos, ensuring that technological design and institutional governance co-evolve under shared values of

accountability, traceability, and adaptive learning.

The study draws on three structured categories of material: regulatory and public documentation; synthetic and simulated logs; drill records and post-exercise reviews. All materials are managed under version-controlled, tamper-evident archival procedures to ensure traceability, auditability, and reconciliation of both technical and institutional components. This methodological design enables the study to simulate realistic governance dynamics while maintaining analytical rigor, providing a reliable foundation for constructing the proposed reference architecture and its validation framework.

2. Literature Review and Theoretical Basis

2.1 Collaborative Governance and Polycentric Governance

Collaborative governance emphasizes consensual, joint public action achieved through institutionalized processes of face-to-face dialogue, information sharing, and collective decision-making among government agencies, market actors, and social organizations. The core tenet of this theory is that the effectiveness of social governance derives from the collective efforts of multiple societal actors. Governance outcomes emerge as collaborative results shaped by the alignment of objectives, negotiated rules, and the integration of resources among public authorities and societal organizations [4].

In policy domains characterized by high uncertainty and interdependence, collaborative governance requires an interactive structure centered on three essential pivots: joint problem definition, shared fact bases, and collective commitment to action. Its operational conditions include a moderate dispersion of authority and resources, the presence of initial trust, a clearly designed process architecture, and sustained neutral facilitation.

Polycentric governance theory, originally developed to address complex collective action problems such as climate change [5], further enriches this understanding. It posits that within complex systems, semi-autonomous decision-making nodes and complementary functional divisions can enhance overall system adaptability and resilience-provided that a set of mutually recognized rule systems and interface standards exists. In the absence of such coherence, systems tend to regress into fragmentation and inefficiency. The polycentric governance framework thus provides analytical leverage for examining coordination and cooperation among diverse actors, supporting the development of more efficient, adaptive, and responsive governance networks [6].

Applied to road emergency management, these theories illuminate two critical insights. First, cross-departmental consensus must be compiled into executable procedural rules-including time constraints, communication standards, and interface specifications-rather than remaining at the level of declarative collaboration. Second, polycentric coordination depends fundamentally on a shared factual view and a version-controlled rule base-precisely the institutional focus of the All-Domain Situational Awareness (All-Domain, SA) framework. Together, these insights provide the theoretical anchor for constructing a resilient, auditable, and cooperative architecture for road emergency governance.

2.2 Resilience Governance and Resilience Engineering

Resilience governance and resilience engineering emphasize the capacity of organizations to absorb, adapt to, and recover swiftly from disruptions. Resilience governance entails not only the expansion of organizational capabilities but also the restructuring of institutional frameworks and paradigm shifts [7]. Anchored in the cyclical model of "prevention-preparedness-response-recovery," its core lies in the proactive delegation of authority, the explicit demarcation of fault-tolerance boundaries, and the institutionalization of review and feedback mechanisms. In the field of engineering, "resilience" refers to the property of materials to regain their original state after deformation under external forces [8]. Resilience engineering, by extension, requires systems to operate in a degraded mode, switch redundancies, isolate fault domains, and maintain observability in contexts such as weak connectivity, network outages, or overload. Moreover, it emphasizes making tacit knowledge explicit through systematic drills and exercises.

More broadly, collaborative and polycentric governance structures provide the institutional

foundation for consensus-building and process design across departments. Both resilience governance and resilience engineering incorporate uncertainty and extreme scenarios into institutionalized authorization and exercise cycles. A survey of the literature on road emergency management from technological and governance perspectives reveals a substantial body of research both domestically and internationally. On the technological front, most studies focus on: (1) information platforms and algorithmic performance within single domains or departments; (2) localized optimization of technological processes, such as incident detection, congestion alerts, and route guidance; and (3) empirical assessments of command and dispatch procedures. From a governance and collaboration perspective, however, policy instruments remain insufficient in facilitating a truly integrated approach to comprehensive situational awareness-one that unites governance, coordination, and resilience in road emergency management.

3. Conceptual Definition and Analytical Framework

3.1 Key Concept Definitions

3.1.1 All-domain situational awareness

Situational awareness entails perceiving a broad array of environmental factors across time and space, comprehending their significance, and projecting their future states. The process of situational awareness is initiated through perception [9]. The cultivation of situational awareness is a critical competency for emergency management personnel and constitutes a foundational prerequisite for effective and successful emergency response [10]. Irrespective of whether a crisis is precipitated by natural or anthropogenic disasters, emergency responders must maintain a comprehensive and accurate perception of pertinent information in order to facilitate coordination and ensure the effective execution of response activities; this represents the starting point for all operations [11].

Within the context of road emergency management, all-domain situational awareness (All-Domain SA) refers to the capability for continuous, multi-source perception and integrative assessment across the road network, transport hubs, tunnels and bridges, service areas, adjacent environments, and low-altitude platforms. It involves institutionalizing the four-stage chain of information-collection, decision-making, execution, and review-through regulatory mechanisms. The governance dimension of this concept is reflected in the translation of "seeing" into executable procedural rules (specifying timeframes, standards, and responsibilities); the incorporation of technological capacities (such as detection, simulation, and guidance) into auditable authorization and accountability structures; and the formalization of technical downgrading under extreme scenarios (such as weak or disconnected networks) as resilience governance clauses and standard operating procedures (SOPs) for designated roles.

3.1.2 Data-governance collaboration

Data governance has the potential to serve as an innovation engine, leveraging data as a critical production factor in the marketplace [12]. Collaborative data governance involves a series of governance actions undertaken by multiple stakeholders with respect to data elements, with the objective of enhancing both data value and governance efficiency [13]. Multiple actors reach contractual agreements on the purpose limitation, minimum necessity, tiered access, lifecycle management, quality assurance, and auditing of data, and these are integrated with the RACI governance matrix. This integration facilitates traceable management across the dimensions of "who shares-what is shared-with whom-for how long-and with what accountability." Organizations may construct collaborative data governance frameworks according to the logical dimensions of "structure-function-mechanism" [14]. International research on collaborative data governance has tended to focus on challenges such as data security and standardization, and it is widely recognized that issues of data standardization significantly affect the effectiveness of cross-institutional collaborative governance [15].

3.2 Common Operating Picture

To enable executable, auditable, and transferable management across the entire chain of "information-decision-execution-review," this study abstracts the fundamental elements of all-domain situational awareness in road emergency management into three core entities: Incident, Resource, and Policy. These are standardized through a unified system of

metadata, semantics, and constraints. Respectively, these entities serve as the primary carriers of data flow, control flow, and policy flow, while their traceable identifiers and relational constraints collectively establish a "Common Operating Picture" (COP).

3.2.1 Incident

An incident refers to an objective event occurring at specific spatiotemporal coordinates that exerts an actual or potential impact on road network operations and public safety. The minimal descriptive unit for an incident is defined as:

Incident = (id, t, loc, type, severity, confidence, evidence)

where *id* is a globally unique identifier; *t* denotes the event timestamp (including the time of detection and verification); *loc* specifies spatial positioning (road code, milestone, coordinates, and affected area); *type* refers to a standardized category (e.g., multi-vehicle collision, hazardous material leakage, tunnel fire, etc.); *severity* indicates the classification level (S0-S3); *confidence* represents the confidence score; and *evidence* provides pointers to supporting materials (such as images, video, or sensor summaries). The incident object serves as the factual carrier within the data flow and is subject to constraints including field-level tiered release, minimum necessity, lifecycle management, and auditability: public-facing data excludes PII and sensitive coordinates, while professional/internal users access fields according to contractual visibility. The incident lifecycle follows the sequence "detection → verification → classification → clearance → review," with each stage linked to a responsible party and a corresponding time threshold.

3.2.2 Resource

A resource refers to any capacity element-such as personnel, vehicles, equipment, and facilities-that can be utilized for response operations and to support decision-making, with an emphasis on observability and dispatchability of capability, status, and location. Its standardized representation is as follows:

Resource = (id, kind, capability, status, loc, owner, availability)

where *kind* indicates the category of resource (e.g., tow truck, ambulance, fire service, UAV, RSU, trailer, etc.); *capability* denotes the list of abilities (such as towing capacity, firefighting grade, flight endurance, sensing modality, etc.); *status* describes the operational state (idle, en route, in operation, malfunction, disabled); *loc* refers to the current location or coverage area; *owner* identifies the entity with ownership and the relevant contact; and *availability* specifies the window of availability and related constraints (e.g., time periods, weather, regulatory requirements). Resource objects are directly coupled with the control flow: dispatch commands target resources, requiring idempotency and receipt acknowledgment; any change in resource status triggers an update of the factual view. Resource information is by default classified for professional or internal use, and fields involving commercial or personal sensitive attributes must be anonymized and strictly logged.

3.2.3 Policy

A policy refers to the formalized and versioned articulation of rules governing actions such as traffic guidance, speed restrictions, closures, diversions, and coordinated rescue efforts under specific scenarios and constraints. Serving as an institutionalized bridge from information to action, its formal definition is:

Policy = (id, scope, preconditions, actions, safeguards, rollback, kpi, version)

where *scope* specifies the applicable road segments, time windows, or scenarios; *preconditions* refer to triggering conditions (such as event type and severity thresholds, weather, or network status); *actions* detail the sequence of operations, including participating entities, authorization levels, and execution order; *safeguards* identify risk controls and exceptions (such as public information standards and minimal impact domains); *rollback* defines the criteria and steps for policy reversal; *kpi* (key performance indicators) outline process and outcome metrics (with only their definitions and data collection methods specified, not measured values); and *version* denotes the semantic versioning (vMAJOR.MINOR.PATCH) along with approval and provenance records. Policy objects carry the policy flow and, through mechanisms for phased rollout, rollback, and provenance, are integrated into the control flow loop to ensure the traceability and consistency of execution responsibilities and communication protocols.

3.3 Relationships between Objects and Governance Semantics

The three aforementioned entities are interconnected through a set of constrained relationships:

First, the triggering relationship: Incident ⇒ Policy (an incident that meets specified preconditions initiates policy orchestration);

Second, the actuation relationship: Policy ⇒ Resource (policies generate instructions and configurations for resources);

Third, the acknowledgment relationship: Resource ⇒ Incident (resource execution feedback updates the incident status and provides evidence for review).

From a governance semantics perspective, incidents serve as evidence, policies as rules, and resource execution as the manifestation of authorization. All three are subject to constraints such as tiered disclosure, minimum necessity, lifecycle management, auditability, and accountability. Cross-departmental semantic alignment and version traceability are achieved through a unified ontology, coding schemes, and metadata directories.

3.4 Two Operational Chains

3.4.1 The incident response chain

The Incident Response Chain is fundamentally constrained by time sensitivity and protocol consistency, with the objective of transforming fragmented information into accountable, coordinated actions within a defined time window. Its basic structure comprises the following stages:

(1) Sense (Detection/Verification): Initial "incident objects" are generated by sensing and reporting entities, such as on-site teams, roadside devices, UAVs, and navigation data sources. The minimal fact unit includes time, location, type, severity, confidence, and evidence pointers, with field-level compliance labeling and unique identification completed at this stage.

(2) Assess (Consultation/Classification): Under governance constraints, cross-departmental merging and conflict resolution of common operating picture data are performed to produce standardized incident classification and impact assessment. This stage utilizes a RACI matrix to clarify "decision-making authority, advisory roles, and information rights," each tied to specific time thresholds.

(3) Command (Tiered Release and Instruction Issuance): In accordance with data sharing agreements, information is disseminated externally in a tiered manner (public/professional/internal/sensitive) and control-flow instructions are issued internally. Policies are derived from the versioned policy flow and scenario library; execution entities are required to acknowledge receipt and maintain idempotent semantics.

(4) Review (Execution Feedback and After-Action Review): Execution results for control flow are logged, generating review entries such as timelines, exception points, protocol deviations, and improvement suggestions. This process also triggers proposals for policy library updates and protocol version revisions.

Consistency within this chain is ensured by a "three-flows × SLA/compliance label" matrix: the data flow carries evidence, the control flow carries authorization and execution, and the policy flow carries rules and versions; each is bound to timeliness, availability, and compliance/retention indicators, respectively. To absorb uncertainty, the chain incorporates a built-in "degradation–fault tolerance–recovery" state machine: when thresholds such as weak connectivity or network disconnection are met, edge authorization and localized SOPs are automatically activated, permitting the delivery of the minimally acceptable service within predefined boundaries, with post-recovery feedback and evidence transmission completed thereafter.

3.4.2 The capability development chain

The Capability Development Chain is primarily constrained by institutional evolvability and portability, aiming to systematize and template operational experience for broader reuse and diffusion across governance domains. Its basic structure includes:

(1) Drill (Exercises and Scripting): Standardized exercise scripts are designed around high-risk scenarios (such as extreme weather, long tunnels, hazardous materials, or hub congestion), with clear specification of triggering conditions, role rosters, minimal data sets, and time thresholds.

(2) Evaluate (Assessment and Audit): Both process and outcome of drills are assessed, focusing on governance KPIs such as timeliness of information dissemination, consensus rate in consultations, coverage rate of acknowledgments, consistency of protocols,

and closure rate of after-action reviews, thereby forming traceable audit records.

(3) Revise (Rule Revision): Evaluation findings are translated into proposed version updates for the "policy library", "protocol repository" and "data sharing agreements." Semantic versioning, together with phased rollout and rollback mechanisms, ensures incremental evolution without undermining existing stability.

(4) Release (Deployment and Activation): Following approval and record-keeping, new versions are released and cross-departmental synchronization is achieved through training and notification systems, thus updating the baseline for the Incident Response Chain.

The Capability Development Chain and the Incident Response Chain are linked through a feedback loop enabled by version governance: after-action review entries from the response chain serve as input for revisions in the capability chain; the updated rules and protocols from the capability chain, in turn, feed back into the policy flow and data sharing agreements of the response chain. In this way, the system achieves continuous optimization of the governance-technology nexus through an iterative process of experience, rules, execution, and feedback.

3.5 Three-flow and Compliance Label

3.5.1 The data flow

Within the aforementioned "three-layer, two-chain" structure, this study abstracts the operational mechanism of all-domain situational awareness in road emergency management as three institutionalized and complementary flows: data flow, control flow, and policy flow. These three flows correspond to the governance semantics of "evidence-authorization-rules": data flow is responsible for factual statements and evidentiary references; control flow embodies named authorization and traceable execution; and policy flow, through a versioned rules system, acts as a mediator, translating facts into actions and subjecting them to post hoc audit. The unification of these flows depends on a tagging system centered on timeliness, availability, and compliance, as well as cross-departmental semantic alignment. This is further reinforced by lifecycle management and record-keeping mechanisms to establish an accountable closed loop.

The fundamental function of data flow is to provide a verifiable common operating picture, encompassing incident alerts, segment operational status, resource availability, and environmental factors, all of which require structured definitions of minimal fact units such as time, location, type, and confidence level. Traditionally, distributed data stream processing systems are used for traffic data, where data flows are assigned to a finite set of processing nodes according to system-defined mapping functions, enabling parallel processing [16]. Distinct from general information management, this study emphasizes that the attributes of compliance, timeliness, and quality must be embedded in the data flow at the point of creation: on one hand, field-level tiered release and the principle of minimum necessity define the visible boundaries of data for different audiences, with the public-facing side by default excluding any personally identifiable information and high-precision sensitive coordinates; on the other hand, the requirement for minute-level response imposes timeliness constraints at the encoding level, assigning data latency classes and availability targets to ensure a consistent service commitment throughout the processes of multi-source aggregation and conflict resolution.

As such, the data flow serves not only as the factual input for the incident response chain but also as the audit evidence for the evaluation stage of the capability development chain. Its lifecycle-from collection, usage, retention, to destruction-must be governed by explicit contractual stipulations, and every access or modification must generate immutable fingerprints and logs.

3.5.2 The control flow

In contrast to the "declarative" function of the data flow, the control flow is tasked with both "execution" and "acknowledgment." The legitimacy of the control flow derives from explicit organizational authorization and defined role responsibilities, while its effectiveness depends on maintaining idempotent semantics and a closed feedback loop once commands reach the execution endpoint. To prevent semantic drift and dilution of accountability during cross-domain dispatch, control instructions should be constrained at the governance layer as structured sets of version-controlled actions, encompassing issuing entities, target objects, spatiotemporal scope, and risk mitigation conditions, and should

institutionalize an observable path of "delivery-activation-acknowledgment."

Scenarios involving weak or disconnected networks do not constitute an interruption of the control flow; rather, they trigger predetermined degradation protocols: at the edge, within the scope of authorized actions, localized SOPs are used to maintain minimally acceptable service levels. All provisional actions are subsequently reconciled with the global factual view through batch reporting upon link restoration. Through this institutionalized chain of "authorization-execution-acknowledgment," the control flow translates interdepartmental consensus into quantifiable behavioral trajectories and provides attributable evidence for subsequent review and after-action analysis.

3.5.3 The policy flow

The policy flow serves as the critical bridge between data and control flows, centering on the versioned management and rollback capability of rules, contingency plans, and scenario libraries. Policy objects should be formalized with elements such as scope of applicability, triggering conditions, action sequences, risk management clauses, and rollback procedures, thereby enabling their migration across governance domains while maintaining semantic consistency. More importantly, the formulation, revision, and release of policies must be incorporated into approval and record-keeping workflows, in order to clearly differentiate the advisory status of "expert recommendations" from the binding status of "policy directives or instructions."

To ensure composable and measurable coherence of the three flows across departments and hierarchical levels, this study introduces a tagging system centered on timeliness, availability, and compliance, which is embedded throughout the object models and interface contracts. Timeliness tags assign permissible latency intervals to various payloads, supporting time-window constraints for consultations and releases; availability tags establish resilience and redundancy requirements for critical links, defined by service-level objectives on a monthly or event-driven basis; compliance tags, at the field level, specify requirements for handling personally identifiable and sensitive information, including retention periods and audit intensity. This tagging system not only supports operational dispatch decisions in real time, but also provides a basis for after-action review and version governance: when discrepancies arise in response chains-such as delays or protocol inconsistencies-the audit system can attribute the deviation to issues in data quality, control execution, or policy selection, thereby clarifying accountability and improvement pathways. The overall governance framework is illustrated in Figure 1.

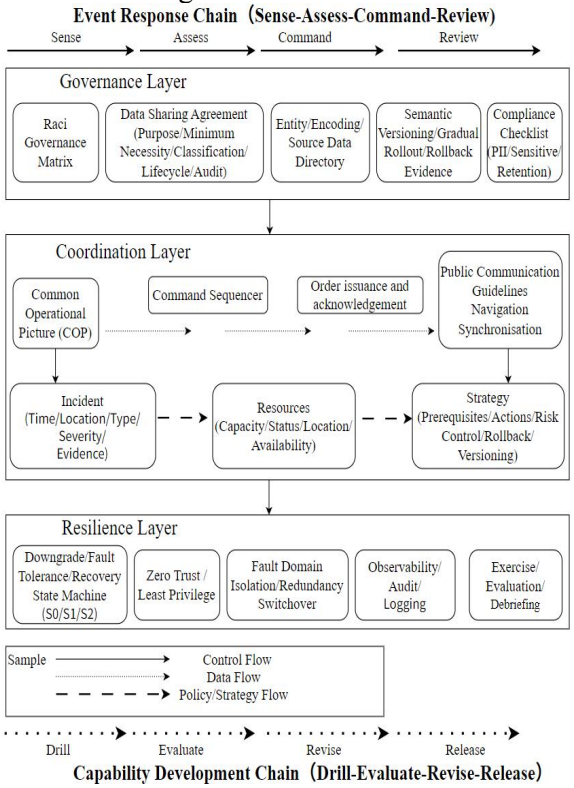

Figure 1. Three- Layer, Two-Chain, Three-Flow Integrated Governance Framework

4. The Data Collaborative Governance

The content of data collaborative governance mechanisms primarily encompasses coordination among actors, objects, platforms, technologies, and institutional arrangements [17]. Cross-departmental collaboration is transformed from "principled consensus" into institutional arrangements that are executable, auditable, and reusable. At the core of this transformation is the use of templated expressions-such as the RACI matrix and Data-Sharing Contract (DSC)-to clearly delineate rights, responsibilities, and boundaries. Public consistency is ensured through tiered disclosure, public communication, and integration with navigation ecosystems. Security and compliance are embedded into both routine operations and extreme scenarios by means of zero-trust, minimum-authorization principles.

Moreover, rule evolution is incorporated into a bounded governance process via semantic versioning, phased rollout, and rollback mechanisms.

4.1 RACI Matrix and DSC Contract Templates

An executable RACI matrix constitutes a procedural contract linked to event sequencing, field-level visibility, and temporal thresholds. Within the incident response chain-comprising detection, verification, classification, release/issuance, acknowledgment, and review-the lead agency bears ultimate responsibility for both external communications and internal directives; traffic police and operational entities are directly accountable for fact generation and resource deployment; specialized departments such as emergency services, healthcare, and meteorology provide consultative input during coordination; and navigation and communications stakeholders are responsible for synchronized dissemination and network assurance. The matrix dynamically adjusts its "responsibility-timeliness-field" triads according to scenario: for instance, in the event of multiple concurrent accidents triggered by extreme weather, the matrix automatically advances the consultative responsibility of meteorological and highway agencies while shortening the consultation window; for tunnel fires, it elevates the direct responsibility and acknowledgment obligations of fire and operations entities. Template-based presentation of the matrix ensures that each cell can be mapped to specific data fields, timeliness levels, and audit points, enabling the system to automatically generate alerts and traceability for expired actions, overreach, or protocol inconsistencies during runtime.

Effective data collaborative governance must facilitate the centralization, standardization, and professionalization of data management [18]. Corresponding to the RACI matrix, the Data-Sharing Contract (DSC) is anchored in field-level constraints and lifecycle management: minimal factual units are generated within T+60 seconds and tagged for timeliness and compliance; professional-side classification and impact assessments are synchronized with the common operating picture within T+5 minutes; and access to sensitive fields is automatically logged for source, purpose, temporal, and spatial boundaries, with immutable attestations generated upon fulfillment of destruction conditions. The templated DSC requires a reusable clause framework-including field visibility matrices, quality thresholds, retention and destruction conditions, access and modification logs, audit sampling, and accountability pathways-so that different regions and institutions can readily adapt the contract with minimal modification, thereby providing a unified, transferable "contract syntax" for domain-level collaboration.

4.2 Tiered Release and Zero-Trust Minimum Authorization

The governance objective of tiered release and public communication is to ensure consistency in source, timing, and messaging across all versions, and to achieve automatic alignment with navigation ecosystem guidance strategies. Upon reaching the release node, the common operating picture generates four levels of expressions-public, professional, internal, and sensitive-according to object attributes and compliance tags, yet all versions remain attached to the same factual snapshot and version identifier. The initial release must be completed within a fixed time window, providing location, impact area, and recommended route in the form of "minimum necessary information"; any subsequent correction window resolves previous discrepancies via "correction notice + version replacement." The navigation ecosystem subscribes to the "authoritative minimum necessary" version through interface contracts, with guidance strategies anchored to the same version number. Any deviation is automatically flagged as an inconsistency event and incorporated into after-action review. This governance arrangement positions "public communication" not as a peripheral technical activity, but as an integral component of collaborative data governance.

Zero-trust minimum authorization is elevated from a technical option to a governance clause. All access to data and control by any actor is evaluated based on the combined factors of identity, device, and context; temporary and emergency authorizations must automatically expire within defined time and spatial boundaries; highly sensitive fields, by default, are presented in de-identified form on the professional side, and can only be decrypted for review upon satisfying both legal basis and

operational necessity, with dual approval and enhanced logging enforced. Weak or disconnected networks are not considered exceptional conditions, but are codified as resilience provisions within the contract: when link quality falls below a threshold, authorized edge personnel may execute local SOPs within the bounds of their authorization to maintain minimum acceptable service; upon restoration, operational logs and evidence chains must be reported within agreed timelines. The binding of fault tolerance waivers and receipt-based attestation both prevents a "paralysis of responsibility" and curbs the normalization of unauthorized actions. During runtime, the audit system continuously monitors the three flows via observability data, automatically registering delays, messaging, and authorization deviations as after-action entries and using them as evidence for the next cycle of rule revision.

4.3 Version Governance

The fundamental objective of version governance is to ensure semantic stability and traceability, constraining changes to policies, protocols, and data contracts within auditable, reversible, and portable boundaries. In terms of semantic modeling, a version is not merely a mechanical file increment but a marker of governance meaning: every change must explicitly define its scope, preconditions, behavioral delta, and compatibility relationships. In operational coupling, version governance must be simultaneously embedded in the data, control, and policy flows. For the data flow, versioning is reflected in schema evolution and changes to compliance tags: following a "backward compatibility first" principle, new fields are introduced as optional, and deleted or renamed fields are managed through alias mapping and dual-write periods, with contract testing at the interface layer preventing destructive releases. In the control flow, versioning manifests as guarantees of action semantics and idempotency: any new instruction must declare idempotency conditions and acknowledgment formats to ensure that, during staged rollout or rollback, terminal state drift does not occur. Policy flow versioning focuses on preconditions and risk control clauses: any new or tightened precondition must be evidenced-linked to corresponding data quality reports and SIA (Situation Impact Assessment) summaries-so that, during after-action review, "why a revision was made" and its consequences can be objectively reconciled.

At the organizational and procurement level, version governance must be externalized into executable contract terms and performance metrics: systems and data services delivered by vendors must support semantic versioning, staged rollout, rollback, and contract testing; key change metrics, such as change failure rates, mean rollback durations, and staged rollout pass rates, should be incorporated into evaluations; and any destructive change leading to cross-domain protocol conflicts or public communication errors must incur contractual liability.

5. The Resilience Reference Framework

A resilience reference framework constitutes a set of explicitly authorized, auditable, and acknowledgeable organizational rules. In this study, the resilience of road emergency management is defined as the institutional capacity to maintain minimally acceptable service levels, ensure risk controllability, and preserve clear accountability within the response chain, even under disturbances such as weak connectivity, network disconnection, system overload, or failures in heterogeneous system coordination.

5.1 State Recognition and Delegated Authorization

The operation of resilience begins with state recognition. The normal state refers to conditions in which information and command channels remain within the agreed thresholds for timeliness and availability, allowing interdepartmental consultations and tiered releases to proceed within standard windows. The degraded connectivity state (weak network) occurs when link quality is reduced, insufficient to support full synchronization but still capable of transmitting key fields and heartbeat signals. In this state, consultations and releases are limited to the minimum necessary facts and incremental policy updates, with execution entities assuming partial orchestration. The disconnected state arises when links are severed or cross-domain communication is unreachable; in such cases, edge personnel operate independently within pre-authorized boundaries, executing local SOPs and recording evidence.

Once the thresholds for degraded or

disconnected states are reached, authorization is automatically delegated to the edge, external messaging shifts to the "authoritative minimum necessary version," and the fault-tolerance waiver is activated. Upon restoration of normal connectivity, the edge must complete acknowledgment and evidence submission within a defined window, and the central authority reconciles version consistency and protocol deviations based on these records.

The boundaries of delegated authorization are defined by the "minimum impact domain" principle, constrained by both task and spatial parameters. In the degraded connectivity state, edge operations may include low-impact actions such as speed restrictions, activation of reversible lanes, ramp control, and localized diversion. In the disconnected state, temporary closures or guidance can be enacted within an even smaller geofenced area, but public communications outside the authorized scope are strictly prohibited. All actions must uphold idempotent semantics to prevent state drift during network restoration or policy reconciliation. The fault-tolerance waiver becomes effective only under the conditions of ex-ante compliance and ex-post acknowledgment: edge operators are exempt from liability when acting according to whitelisted actions and SOPs, but exemption is immediately revoked and accountability procedures are triggered if actions exceed the whitelist or acknowledgments are not submitted on time.

5.2 Engineering Cornerstones

Fault domain isolation and redundant switching are engineering cornerstones of resilience, yet institutionally they must be underpinned by clearly defined takeover relationships and boundary responsibilities. When upstream domains experience functional degradation, neighboring domains' interventions should be strictly limited to the minimum necessary actions for traffic guidance and safety assurance, explicitly excluding the proactive retrieval of sensitive upstream data. The initiation, continuation, and termination of such takeovers are automatically triggered by pre-established thresholds and recorded by the system, eliminating the need for ad hoc coordination or additional approval. To prevent redundancy from resulting in "multiple sources and protocols," the resilience framework stipulates that all external communications during takeover continue to reference the lead agency's "authoritative minimum necessary version," with neighboring domains responsible solely for mirrored dissemination and channel amplification, thereby avoiding the emergence of multiple "authoritative" sources.

The resilience framework mandates the scripting of typical high-risk scenarios, with safeguard indicators functioning as operational thresholds: metrics such as public release latency, navigation alignment rate, inconsistency event count, acknowledgment coverage rate, and rollback trigger rate are defined as "switch variables"-any threshold breach triggers rollback or system expansion. Both drills and actual incident assessment reports must cite corresponding evidence snapshots and tracking IDs to ensure the verifiability of success or failure judgments; revision proposals resulting from these evaluations are incorporated into the version governance process, initially deployed in a limited domain under phased rollout, and expanded upon meeting criteria. This establishes an endogenous cycle of "experience-rule-execution-acknowledgment-review-revision-re-release."

5.3 Risk Point Control

Coupling with public communication represents a critical risk point for resilience. Weak connectivity and network disconnection often coincide with the spread of rumors and misinformation; in such degraded states, public messaging is reduced to the minimum necessary information-location segment, impact area, and recommended route-accompanied by a status indicator for "degraded operation." Upon restoration of connectivity, a correction window is immediately initiated, replacing earlier communications with a "correction notice + version replacement." The navigation ecosystem aligns automatically via version recognition. Any deviations across channels are logged by the system as inconsistency events and are incorporated into accountability or improvement processes during after-action review.

The resilience framework employs version governance as its institutional track, ensuring that downgrade protocols and rollback pathways are transferable, traceable, and reversible. Each set of localized SOPs is

published with a semantic version, specifying triggering conditions, authorization boundaries, action sequences, and rollback steps. Phased rollouts are restricted to specific segments, time windows, or event types, and any breach of safeguard indicators triggers immediate rollback without requiring additional approval. Rollback encompasses not only technical reversals but also coordinated terminal actions and public communication corrections, all adhering to the minimum impact domain principle to avoid systemic disruption. Through this governance-driven approach, resilience is transformed from a matter of "engineering redundancy" into an "organizational capability," thereby ensuring both safety and compliance, providing a stable baseline for minute-level emergency collaboration, and enabling a sustainable path for continuous improvement.

6. Policy Pathways and Conclusions

The policy design pathway should follow the axis of "Minimum Viable Collaborative Unit (MVCU) → corridor-level expansion → domain-wide rollout," adhering to a progressive logic that moves "from point to surface, from light to heavy, from contractual to regulatory." The MVCU centers on a high-incident node or critical hub, assembling the minimum viable data set, role set, and interface set into an operational closed loop: minimal fact units and compliance tags are co-generated by traffic police and operators, the lead agency issues the authoritative minimum necessary version within a fixed window, the navigation ecosystem aligns through version synchronization, and acknowledgment and after-action review are completed in short cycles. Two to three scenario-based drills are conducted to test executability and accountability, producing the first batch of institutionalized artifacts: localized RACI–DSC templates, tiered release protocol libraries, authorization and acknowledgment formats, version governance processes, and conditions for phased rollout or rollback.

The effectiveness of the policy advancement path depends on the internalization of evaluation and accountability. Governance KPIs are used as methods, not as "performance displays": metrics such as release timeliness, consultation consensus rate, acknowledgment coverage, and review closure rate are to be used alongside structural indicators like correction window utilization, inconsistency events, version rollbacks, and phased rollout pass rates, to avoid speed metrics crowding out accuracy and safety. Assessments are based on operational logs and records, conducted by third parties or cross-departmental audit teams. Accountability follows the principles of "clear responsibility interface-pre-positioned fault tolerance clauses-effective correction mechanisms," prioritizing revisions for deviations caused by systemic flaws, and imposing explicit penalties for willful breaches of contract or repeated inconsistencies.

The governance framework proposed in this study is structured as "three layers-two chains-three flows," and utilizes tools such as RACI, DSC, tiered release, zero trust, and version governance, advancing cross-departmental collaboration from "visibility" to "executability," from "executability" to "auditability," and ultimately to "reformability." Its portability stems from templating and versioning: unified object models, field semantics, and contract syntax enable rapid adaptation across regions with minimal modification. Its stability derives from resilience clauses and rollback mechanisms: weak connectivity and disconnections are regarded as endogenous institutional scenarios, with temporary authorizations and fault-tolerance waivers operating within defined boundaries. Its extensibility is ensured by the MVCU→domain-level policy path, facilitating iterative updates to capability building and rule evolution through continuous drills and after-action reviews.

Future work may proceed along two lines: first, further refining evaluation norms and responsibility interfaces through institutionalized integration with digital twins and industry-scale models, incorporating model outputs into the approval and attestation process of the policy flow; second, exploring "minimum common contracts" for cross-provincial mutual recognition, thus advancing unified protocols and interoperability for the national expressway backbone. Through these pathways, the governance system can maintain alignment of "awareness-decision-execution-review" within a unified semantic and accountability framework, continuously enhancing the public value and social trust of road emergency management.

Acknowledgments

This paper is supported by the Key R&D Program (Soft Science Project) of Shandong Province, China (No.2025RZB0405).

References

[1] Endsley M. R. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37, 1995(37):32-64.

[2] Asante K., Owen R., Williamson G. Governance of New Product Development and Perceptions of Responsible Innovation in the Financial Sector: Insights from an Ethnographic Case Study. Journal of Responsible Innovation, 2014(1):9-30.

[3] Rodrı´guez H., Fisher E., Schuurbiers D. Integrating Science and Society in European Framework Programmes: Trends in Project-level Solicitations. Research Policy, 2013(5):1126-1137.

[4] Parker C F, Nohrstedt D, Baird J, et al. Collaborative Crisis Management: a Plausibility Probe of Core Assumptions. Policy and Society, 2020, 39(4): 510-529.

[5] Ostrom E. A general framework for analyzing sustainability of social-ecological systems. Science, 2009, 325(5939):419-422.

[6] Chen J L, Wang Y N. Research on multi-governance of social responsibility of platform enterprises. Modern Management Science, 2021(7):74-82.

[7] Qi Xiaoliang. Resilient Governance: The Logical Shift and Practical Path of Public Security Governance in Megacities. Urban Development Studies, 2025, 32(9):139-144.

[8] LinXue. An Interpretative Discourse Analysis of Resilient City Policies in China in a Risk Governance Framework. JOURNAL OF SJTU (Philosophy and Social Sciences), 2025, 33(182):33-48+63.

[9] Endsley M.R. Design and Evaluation for Situation Awareness Enhancement. In: Proceedings of the human factors society annual meeting, SAGE Publications, Los Angeles, 1988, 32(2):97-101.

[10] Rao R. R., Eisenberg J., Schmitt, T. (Eds)., Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response and Recovery. The National Academies Press. Washington, DC, 2007.

[11] Schmidt K. The Problem with “Awareness”. Introductory Remarks on “Awareness in CSCW”, Computer Supported Cooperative Work (CSCW): The Journal of Collaborative Computing, 2002, 11(3-4):285-298.

[12] Zhou Yi, Bai Xuerui. Research on Data Collaborative Governance Mechanisms Driven by Application Scenarios. Information Studies: Theory & Application, 2025, 48(11):49-56.

[13] Hu Feng, Wang Bing, Zhang Siqian. From Boundary Division to Cross-boundary Conjugation: A Scan of Interaction Dilemmas and Relief Paths for Government Data col-laborative Governance. E-Government, 2023(4):93-105.

[14] Ye Zhanbei. Practical Promotion and Collaborative Logic of Government Data Governance: A Case Study of N City. Chinese Public Administration, 2021(6):44-49.

[15] Brandell E. E., Strom D. J., Van deelen T. R, et al. A call to Action: Standardizing White-tailed Deer Harvest Data in the Midwestern United States and Implications for Quantitative Analysis and Disease Management. Frontiers in Ecology and Evolution, 2022(10):943411.

[16] Tang Yingfeng, Chen Shiping. Modeling and Solution for Load Balancing Optimization in Distributed Stream Processing System Management. Operations Research and Management Science, 2021, 30(4):155-162.

[17] Zhou Xia, Gu Ying, Chen Weidong,et al.Research on Influencing Factors and Driving-dependence mechanisms of government data collaborative governance .Information Science, 2025,43(2):67-75+148.

[18] Huang Yue, Li Dewei, Xu Enhua. Research on Smart Travel Service Data System for High-speed Railway Passengers. Railway Transport and Economy, 2024, 46(6):87-96.

