Source Oriented Safety Governance for Civil Unmanned Aerial Vehicles in Urban Low Altitude Airspace

Yong Zhang[1,2]*
[1]School of Public Order, People's Public Security University of China, Beijing 100038, China
[2]Center for Low-Altitude Safety Research, People's Public Security University of China, Beijing 100038, China
Corresponding author: Yong Zhang (e-mail: zhangyong@ppsuc.edu.cn).

ABSTRACT The growth of the low-altitude economy has turned urban airspace below 1000 m into a busy, safety-critical operating environment for unmanned aerial vehicle (UAV). Governance today is largely reactive: violations are detected and responses dispatched only once an incident is already under way. Such a model copes badly as traffic density rises and as UAV become more autonomous, harder to detect, and more varied in payload. This paper sets out a source-oriented governance framework that treats four interacting elements—operators, platforms, the airspace environment, and institutions—as a single coupled system. For the operator dimension, we examine how a de-professionalised and geographically scattered user base reshapes risk, and we build a four-layer intelligent model for assessing human-factor risk. For the platform dimension, we argue for moving protection from a bolt-on layer to a designed-in property, achieved through a security-gene embedding scheme and an integrated sense–communicate–navigate–control security chip. For the environment dimension, we describe the layered and zoned structure of urban low-altitude airspace together with a digital, rule-based constraint scheme that turns regulatory text into machine-executable rules. For the institutional dimension, we propose whole-lifecycle UAV management supported by a consortium-blockchain record system (UAV-BCLR) and a governance regime for counter-UAS equipment, linked by a mechanism that couples rules with technical enforcement. The framework shifts governance away from after-the-fact disposal and toward prevention at the logical origin of risk, and it offers theoretical and engineering guidance for an urban low-altitude safety system.

INDEX TERMS low-altitude economy; low-altitude safety; unmanned aerial vehicles; source-oriented safety governance

I. INTRODUCTION

Within roughly a decade, civil unmanned aerial vehicle (UAV) have changed from a niche tool for aerial photography into a general-purpose platform used in parcel delivery, infrastructure inspection, agricultural protection, and emergency response. National and municipal authorities are now opening low-altitude airspace and building unmanned aircraft system traffic management (UTM) capacity so that routine beyond-visual-line-of-sight flight below 1000 m becomes feasible [1]. The very openness that enables legitimate operations, however, simultaneously facilitates non-cooperative and malicious intrusions. Consequently, the convenience afforded by drone services is accompanied by a broad spectrum of security, privacy, and public-safety risks — including accidental collisions, unauthorized surveillance, illicit smuggling, and targeted attacks on sensitive infrastructure [2].

Urban low-altitude safety is, fundamentally, a systems engineering challenge—shaped by diverse stakeholders, heterogeneous technologies, and multifaceted operational use cases. Its associated hazards rarely stem from a single root cause; rather, they arise from the complex interplay among dispersed operators, heterogeneous equipment, operationally demanding environments, and fragmented institutional frameworks. Current mitigation strategies remain predominantly reactive: monitoring, law enforcement dispatch, and on-site incident response are typically initiated only after a regulatory violation occurs or an accident has taken place. While this approach proved viable under conditions of relatively low air traffic volume, it is inherently non-scalable. The cost of continuous, real-time surveillance and rapid intervention increases sharply with rising traffic density. Moreover, the ongoing advancement of UAV capabilitiesincluding enhanced autonomy, reduced detectability, and expanded payload capacity.

Research on UAV low-altitude safety has progressed along several tracks that have developed largely in parallel. One concerns airspace integration and traffic management.

The United States UTM concept of operations and Europe's U-space concept [3] each describe how large UAV populations can be admitted to low-altitude airspace through highly digitalised, automated services, while complementary work has mapped the ecosystem, market, and operational hurdles of urban air mobility [4], [5] and argued for treating low-altitude airspace as the foundation of future urban air transport [6].

A second track addresses the security, privacy, and safety of civil drones and of the emerging Internet of Drones, with a recurring message that protection should be engineered into the platform rather than added afterwards [7], [8]. A third develops detection and counter-UAS technology based on radar, radio-frequency, acoustic, and electro-optical sensing and their fusion [9], [10], [11], supported by broad surveys of counter-UAS systems and of attack-and-neutralisation techniques [12], [13], [14]. Beneath these efforts, systems-theoretic accident models reframe safety as an emergent control property of a layered socio-technical system rather than the simple absence of component failure [15].

Despite this breadth, much international work stays technology-centred and reactive: it concentrates on spotting and removing threats after they appear, and it tends to study a sensor, a protocol, or a regulation on its own rather than as parts of one system. In parallel, researchers have proposed a low-altitude intelligent network that fuses communication, navigation, sensing, and computing to support large-scale operation [16], and have argued that low-altitude airspace should be planned as a strategic spatial resource [17]. Related studies examine how urban low-altitude airspace can be coordinated with surface and subsurface space under UAV traffic demand [18], as well as the build-out of low-altitude infrastructure and public air routes. On the institutional side, China's Interim Regulations on the Administration of Unmanned Aircraft Flight [19] established a nationwide classification-and-grading baseline, and domestic research has accordingly stressed airspace-resource development, new infrastructure, and the macro-level economic and regulatory framing of low-altitude activity.

Three gaps run across this literature. The orientation is mostly reactive, so intervention comes only after a violation and scales poorly with traffic. Work is fragmented by element and by technology, so human-factor, platform, environmental, and institutional measures are rarely combined into one coherent system. And few studies pursue whole-lifecycle prevention that removes risk at its logical origin. These gaps motivate the present work.

We argue that urban UAV safety governance must complete a shift from after-the-fact disposal to source prevention. Every serious accident is preceded by a far larger population of minor incidents and latent hazards [20], so cutting the chance of severe outcomes means acting on the large submerged base of systemic hazards rather than on the visible tip. Systems-theoretic accident models support this reading: they treat safety not as the absence of component failures but as an emergent control property of a layered socio-technical system, in which accidents follow from inadequate enforcement of safety constraints across that hierarchy. By source prevention we mean proactive, whole-lifecycle control of the four governing elements, so that hazards are neutralised before they turn into accidents.

On this basis the paper offers three contributions. First, it formalises a human–machine–environment–management (HMEM) framework that treats the four elements as one dynamically coupled system. Second, it develops a concrete source-prevention pathway for each element: a four-layer intelligent human-factor risk-assessment model; an endogenous security-gene and integrated-chip architecture for the platform; a digital rule-based airspace-constraint scheme; and a consortium-blockchain lifecycle record paired with a counter-UAV governance regime. Third, it specifies a coupling mechanism that renders institutional rules machine-executable.

The remainder of the paper follows the HMEM framework. Section 2 sets out the element composition of the low-altitude safety system, the role of new low-altitude infrastructure, and the case for source-oriented governance. Sections 3 to 6 develop the governance pathway for the human, machine, environment, and management elements in turn, and Section 7 concludes.

II. A HUMAN–MACHINE–ENVIRONMENT–MANAGEMENT FRAMEWORK FOR LOW-ALTITUDE SAFETY

A. ELEMENT COMPOSITION OF THE LOW-ALTITUDE SAFETY SYSTEM

The HMEM framework grows out of man–machine systems engineering in the safety sciences, where it has become a standard instrument for full-element risk identification in high-hazard fields such as industrial, aviation, and nuclear safety. It separates the safety risk of a complex system into four related elements. The human element covers the behaviour and cognition of the acting subject; the machine element covers the state and performance of technical equipment; the environment element covers the external conditions and constraints of operation; and the management element covers the institutions and mechanisms that keep operation orderly. As Figure 1 shows, these are not static, isolated categories but a dynamically interacting network, in which loss of control of any one element can propagate through inter-element coupling and trigger cascading risk.

The human element is the most direct and basic source of risk, and it includes every subject tied to flight activity: operators above all, but also dispatchers and operational managers. Because the operator population is geographically dispersed and exhibits significant heterogeneity in skill level, human factors constitute the predominant contributor to UAV safety incidents. It is therefore essential to distinguish between two distinct categories of human-related risk: negligent risk and malicious risk.

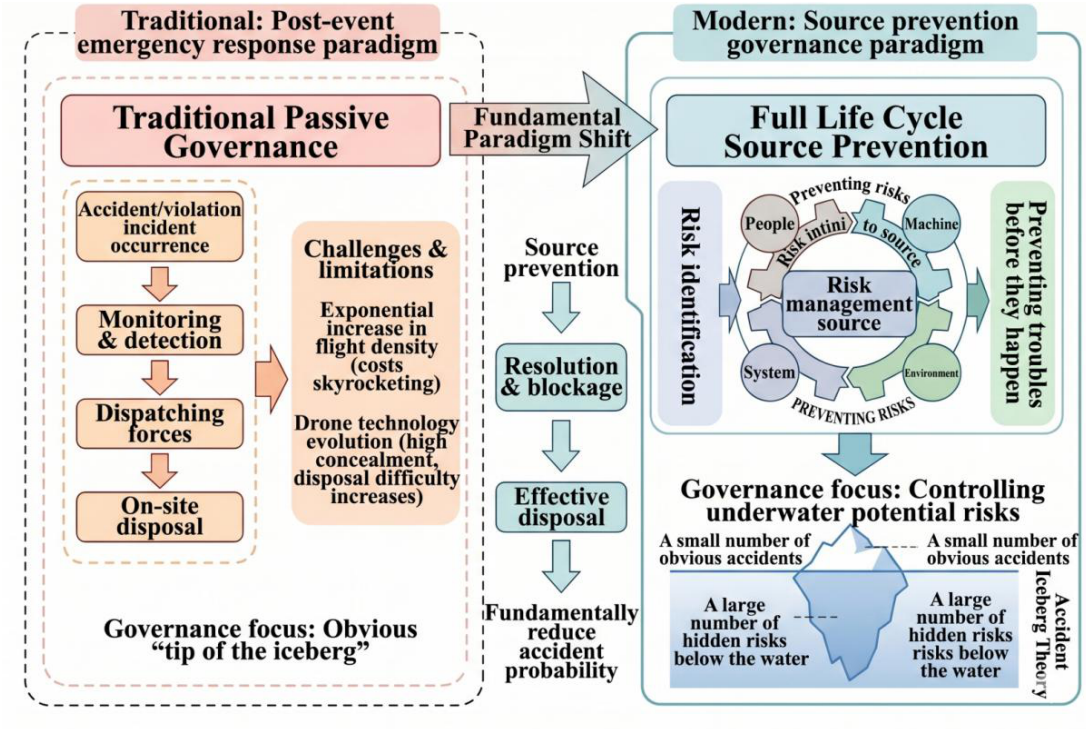

FIGURE 1. The paradigm shift in low-altitude safety governance.

The risk of negligence stems from skill deficiencies, lack of legal awareness, or misjudgment of the operating environment. It manifests itself in unintentional violations of regulations, control errors, and improper handling of emergency situations. In contrast, the risk of malice originates from deliberate and illegal intentions. It is manifested by unauthorized unmanned flight, anti-monitoring modifications, and the weaponization or illegal use of drones,such as for espionage, smuggling, or terrorist activities. Given the fundamental differences in the causes and responses of these two types of risks, different targeted measures must be adopted and handled separately in the design of critical safety systems.

The machine elements form the secure physical foundation. Their risk spectrum encompasses four dimensions: reliability of the mechanical structure and materials, stability of the flight control system, intelligent perception and obstacle avoidance capabilities, and load safety. In urban environments with high density of buildings, battery thermal management is particularly crucial: under mechanical, electrical, or thermal abuse conditions, lithium-ion cells can enter self-sustaining exothermic reactions, ultimately leading to thermal runaway, fire, and explosion [21]. Defects in flight-control logic, incompatible inter-system protocols, and sensor-fusion errors can likewise produce wrong decisions in complex settings, while limited sensing range and degraded performance in low visibility leave a residual closed-loop collision risk in "urban canyons."

The environment element is the spatial field in which UAVs fly and the medium through which risk is induced, amplified, and transmitted. We analyse it along physical, electromagnetic, meteorological, and airspace dimensions. Existing systems for urban spatial planning, spectrum management, meteorological observation, and air-traffic management were designed for ground transport, terrestrial communication, high-altitude flight, or manned aviation, which leaves the low-altitude layer a systemic blind spot. Building occlusion creates multipath effects that can degrade satellite-navigation accuracy from sub-metre to tens of metres; the 2.4 GHz and 5.8 GHz control bands are crowded with Wi-Fi and Bluetooth traffic; near-ground weather needs metre-scale forecast resolution that conventional kilometre-scale numerical prediction cannot deliver; and below 300 m there is neither adequate flight-service provision nor effective surveillance, so many flights remain unseen and unmanaged.

Beyond accidental interference, UAVs face deliberate navigation spoofing. An adversary can inject counterfeit signals that pull a UAV off its planned route without setting off any alarm, a vulnerability demonstrated in controlled capture-and-control experiments [22] and increasingly countered by signal-and learning-based spoofing-detection methods for UAV [23].

The management element is the institutional guarantee of safety. It spans the full chain from standards and administrative licensing, through operational surveillance and enforcement, to penalties and the handling of public opinion. China has issued the Interim Regulations on the Administration of Unmanned Aircraft Flight together with supporting product-safety standards, yet a standards system covering all elements and all scenarios is still being built.

Coordination across public security, military aviation, civil aviation, industry, and market regulation remains hampered by departmental silos, isolated information, and unclear responsibilities, all of which limit collaborative governance.

B. NEW LOW-ALTITUDE INFRASTRUCTURE AS THE CARRIER OF GOVERNANCE CAPABILITY

New low-altitude infrastructure is the core of the environment element. It is at once the physical support for operation and the technical carrier of supervisory capability, and it forms the substrate of the low-altitude intelligent network that fuses sensing, communication, navigation, and computing for large-scale operation. It comprises perception-and-monitoring facilities, namely operation-identification receivers, low-altitude detection radar networks, radio-spectrum sensing, electro-optical monitoring, and acoustic nodes, that together act as a perception nervous system for the urban sky; communication-and-navigation facilities that secure link reliability and anti-jamming capability; take-off-and-landing facilities such as vertiports and drone nests; and meteorological facilities that provide metre-scale forecasting and risk warning.

As Figure 2 indicates, the contribution of this infrastructure can be read as a sense–identify–counter chain. Sensing comes first. Coordinated deployment of radar, radio-frequency sensing, electro-optical, and acoustic modalities enables three-dimensional perception across the whole domain and around the clock, and multimodal fusion raises the chance of detecting even non-cooperative targets that emit no response signal. The trade-offs among modalities are well documented. Radar reaches long range but struggles with the small radar cross-section of consumer UAVs; radio-frequency sensing passively classifies drones and can localise the operator [10]; and acoustic sensing penetrates geometric obstructions but is swamped by urban background noise beyond short range. Reviews of unauthorized drone detection and multimodal classification consistently emphasize that sensor fusion, rather than reliance on any single modality, constitutes the most effective approach for reliable identification [24].

In the identification stage, low-altitude digital maps, three-dimensional airspace models, and the flight service platform jointly form an integrated situational awareness picture. The analysis of flight tracks and behavior patterns by artificial intelligence transforms passive human discovery into active machine prediction. It promptly issues warnings for high-risk and high-threat flight behaviors, and takes appropriate countermeasures when necessary.

In the countermeasure stage, the linkage between the flight service platform and anti-drone equipment can implement graded intervention for identified threats. The current development status of anti-drone systems covers technologies such as radio high-power suppression, navigation deception, net capture, laser, and microwave [10]. Two practical shortcomings still exist: the fragmentation of standards among different manufacturers' equipment and the incompatibility of data formats cause information islands; the countermeasure facilities are concentrated in core urban areas, and there are secondary disaster problems in countermeasures, such as interfering with normal radio facilities.

C. THE RATIONALE FOR SOURCE-ORIENTED GOVERNANCE

For human elements, the key lies in cultivating a group of qualified operators and establishing a law-abiding aviation culture. This is achieved through hierarchical training and qualification certification, linking violation records and accident responsibilities to flight permissions in a dynamic lifetime credit management system, as well as focusing on the key tracking of high-risk entities. For machine elements, the focus is on the inherent technical reliability of in-use platforms - through incorporating flight stability, obstacle avoidance, electronic fences, and remote identification into mandatory certification requirements of mandatory product safety standards, as well as full life-cycle safety archives for key components. For environmental elements, the focus is on forming comprehensive, precise, and reliable perception and guarantee capabilities centered on new infrastructure, accompanied by refined low-altitude weather services, electromagnetic environmental protection, and scientifically delineated no-fly, restricted-fly, and permitted-fly zones. For management elements, the focus is on building a system with clear rights and responsibilities, efficient collaboration, and complete legal systems.

III. HUMAN-FACTOR SAFETY GOVERNANCE

A. RISK CHARACTERISTICS AND INDUCEMENT MECHANISMS

Compared with manned aviation, the UAV operator population is much more widespread and dispersed, which in turn reshapes both how human-factor risk is distributed and how it evolves. Operators can be divided into two groups. Professional operators—such as commercial aerial-photography pilots as well as logistics, agricultural, and emergency operators—are usually trained and licensed in a systematic way. Consumer users make up a huge and fast-growing group with uneven levels of training, and many of them fly without certification. Their risk behaviour can be grouped into four types: skill-deficiency risk, rule-indifference risk, situational-misjudgement risk, and malicious-operation risk. The first three largely arise from insufficient competence or awareness; the last involves intentional, subjectively malicious actions, and it falls within the criminal domain.

As Figure 3 shows, human-factor risk is best understood across individual, organisational, and system levels. At the individual level, cognitive-load theory suggests that when the information an operator needs to process goes beyond cognitive capacity, real demands for any task that combines hand–eye coordination with spatial perception make attention lapses and judgement errors more likely. In addition, fatigue, emotion, and stress further degrade performance. At the organisational level, an operator's safety is shaped

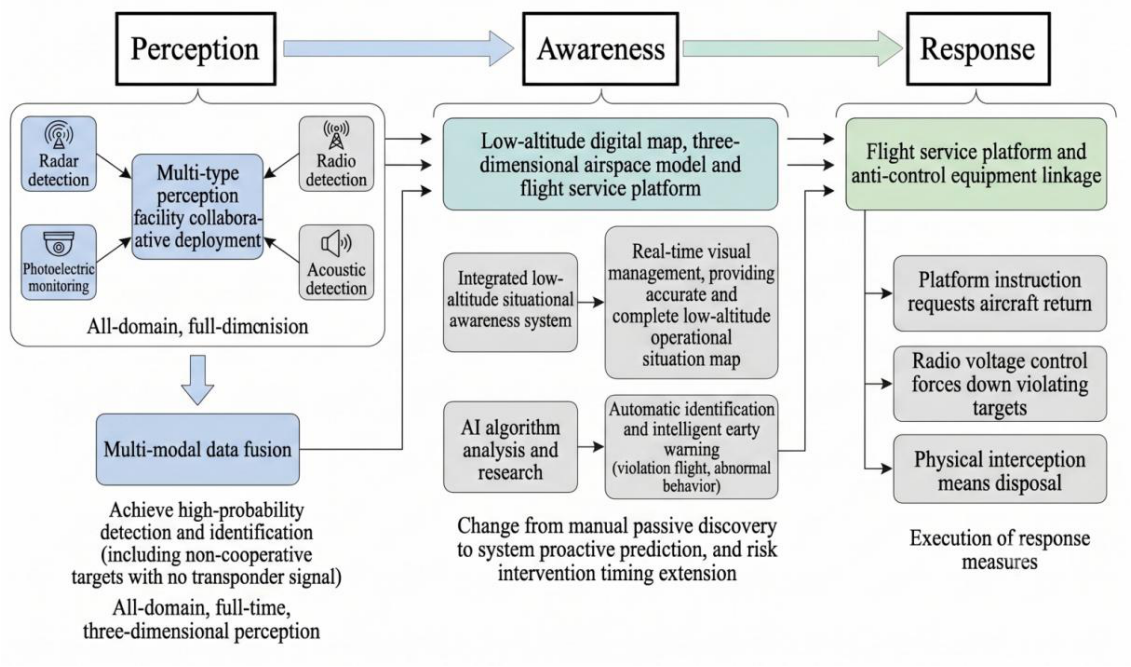

FIGURE 2. How new low-altitude infrastructure supports urban low-altitude safety governance.

by the operating company's safety culture, training, and supervision, where a "use-heavy, training-light" approach undermines both competence and awareness. At the system level, shortcomings in regulation, weak enforcement, and outdated technical means together create the conditions in which human-factor risk takes root. This multilevel view—where latent organisational and systemic conditions come before active operator errors — is the core message of modern human-error research [26].

Technological change also adds a new dimension. As autonomy increases and the operator's role shifts from direct controller to task supervisor, skills can decline and situational awareness can fade. As a result, when automation fails or encounters conditions beyond its competence, an operator who has been removed for some time from manual control may be unable to intervene.

B. CAPABILITY ADMISSION, ASSESSMENT, AND BEHAVIOURAL NORMS

Scientifically based qualification management is the key tool for managing human-factor risk at its source. The Interim Regulations on the Administration of Unmanned Aircraft Flight establish a classification-and-grading structure, with qualification requirements that vary according to risk level. In terms of classification, qualifications should correspond to the platform type, because multirotor, fixed-wing, unmanned helicopter, and electric vertical take-off and landing (eVTOL) aircraft differ in control principles, flight characteristics, and emergency procedures, as well as across the micro, light, small, medium, and large weight categories. In terms of grading, the qualification level should be aligned with the operator's skills relative to the complexity of the tasks involved.

Qualification management should extend beyond initial entry and continue throughout the operator's career through a dynamic assessment system. Entry assessment may combine a theory exam, practical skills testing, and psychological evaluation, while ongoing re-training and re-assessment helps to follow technical and regulatory changes. A unified national flight-record system that captures each operator's flight hours, operating areas, violations, and accident history would produce an objective credit profile—making re-evaluation easier for compliant operators and, for those with repeated violations or responsible accidents, triggering restrictions, mandatory training, or even revocation.

Training should be differentiated. Consumer users benefit most from emphasis on what must not be done and on emergency handling, whereas professional operators need systematic, scenario-specific curricula; embedding a basic-training requirement at the point of sale, as a precondition for activation, closes a control gap in the distribution chain. Behavioural norms then put these requirements into practice across pre-flight preparation (environmental assessment, equipment inspection, mission planning), in-flight conduct (safe separation, visual observation, link monitoring, and avoidance of high-risk manoeuvres), and post-flight review (record-keeping, anomaly analysis, and lesson extraction).

C. AN INTELLIGENT HUMAN-FACTOR RISK-ASSESSMENT MODEL

Quantitative assessment of human-factor risk is the core technical support for precise governance of flight subjects. Traditional human-factor methods, largely carried over from manned aviation, tend to be static, subjective, and limited by

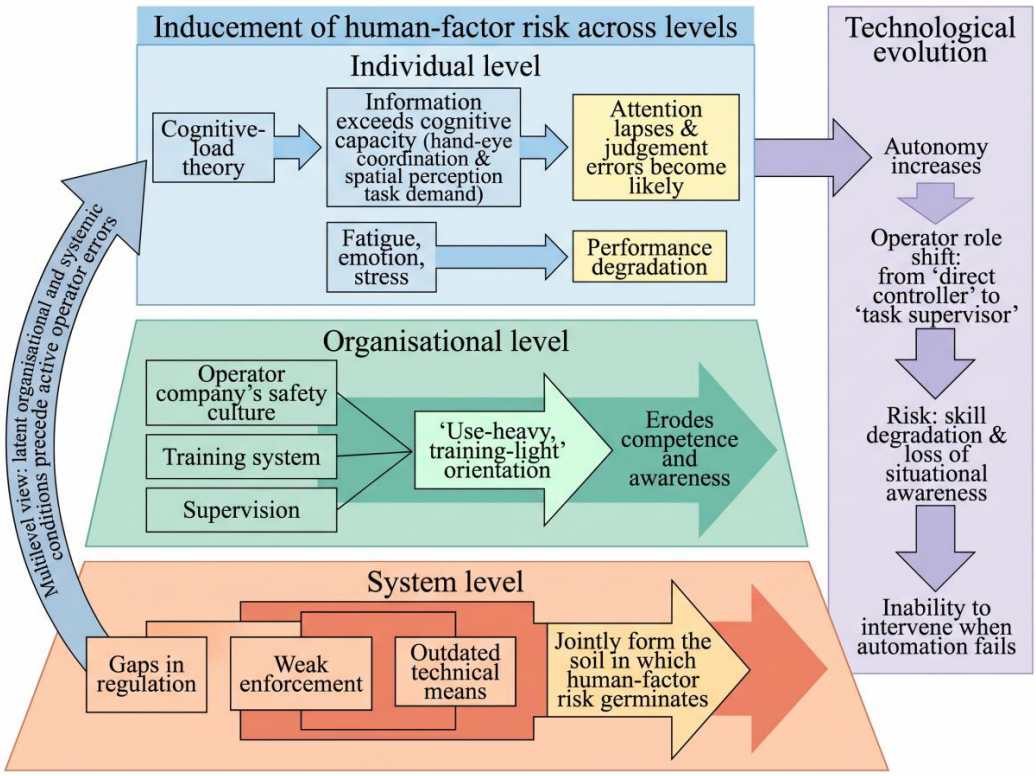

FIGURE 3. The integrated human-factor risk model.

sample size. We therefore build a model that combines classical human-factors engineering with artificial-intelligence techniques and that achieves real-time quantification, trend prediction, and graded control through multi-source data fusion and dynamic weighting.

The model uses a four-layer progressive architecture. A data-acquisition layer integrates heterogeneous data from the regulatory platform, flight terminals, the training system, and third-party databases. A feature-extraction layer cleans, transforms, and engineers features that reflect human-factor risk. A risk-computation layer combines weighted summation with dynamic adjustment to compute a composite risk value and predict its trend. A decision-support layer outputs graded warnings and targeted interventions. Through literature analysis, expert interviews, and the Delphi method, we establish a hierarchical indicator system of four first-level, twelve second-level, and thirty-six third-level indicators, all standardised on a 0–100 scale in which higher values denote higher risk, and we compute a base risk value by hierarchical weighted summation in which the initial weights serve only as baseline parameters.

Because the relative importance of different risks shifts sharply across scenarios, with rule-indifference risk dominating near airport clearance zones and situational-misjudgement risk dominating in complex urban settings, a fixed-weight model is inadequate. The model therefore adds an attention-based neural network that takes a scenario feature vector (area type, UAV category, mission type, population density) as input and outputs dynamic first-and second-level weights, drawing on the capacity of attention mechanisms to allocate representational emphasis adaptively across inputs [27]. Because human-factor risk evolves with skill, psychological state, and behaviour, the model also uses a long short-term memory (LSTM) network, which is well suited to capturing long-range dependencies in time series [28], to forecast the risk trajectory over the next three months from the preceding six months of monthly risk values, flight-hour changes, and violation records.

The base, dynamically adjusted, and predicted values are then fused, with fusion coefficients tuned by grid search, into a final composite human-factor risk value. This value is mapped to five grades, namely low (0–20), general (21–40), medium (41–60), higher (61–80), and high (81–100), each tied to a matching intensity of supervision and intervention, from routine annual re-evaluation through to qualification revocation and industry blacklisting.

IV. INTRINSIC SAFETY GOVERNANCE OF THE UAV PLATFORM

A. FROM EMBEDDED PROTECTION TO ENDOGENOUS PROTECTION

Unlike safety models that lean on external supervision and after-the-fact disposal, intrinsic-safety governance places safety capability inside the UAV itself, building a technical system that carries "safety genes" by design. Platform protection has been moving from an external add-on toward

a native, built-in property, a shift that mirrors the wider move from remediation to source prevention.

The prevailing embedded-protection mode folds safety-control functions such as geofencing, real-name registration, and activation control into the flight-control loop through software embedding and firmware upgrades. It gives source governance a basic technical foundation, but its limits are inherent. Safety and core flight functions are decoupled, so the control module sits as an add-on that skilled actors can crack or bypass; protective depth is thin against increasingly sophisticated threats; and functional upgrades depend on vendor firmware pushes, with the latency and incomplete coverage that this implies.

The endogenous-protection mode instead writes safety-control genes natively into the core architecture and couples safety capability tightly with the UAV's perception, communication, navigation, and control functions. From the hardware and system-architecture level upward, it builds a native protective mechanism that cannot be modified, bypassed, or disabled. Safety and flight functions are physically fused at the chip-architecture level, so even an attacker with physical control cannot strip out the safety module. Core safety parameters and control rules are cured in encrypted form inside a dedicated secure chip, and any attempt to alter them triggers a protective state or an automatic return-to-home.

Two more properties are important. The safety functions operate independently of any external commands and of network connectivity, so the built-in mechanisms continue to work even if communication is lost. At the same time, the system can adapt its safety strategy based on the operating environment, the mission, and the level of risk. This approach aligns with a wide consensus in the drone-security literature that security should be a central, designed-in attribute rather than something added on later.

B. THE SECURITY-GENE EMBEDDING MECHANISM

By analogy with biology, the security gene determines a UAV's safety phenotype and underlies its safe behaviour. Each UAV is assigned a globally unique identity, comparable to a vehicle identification number or an IMEI, written into the secure chip during production and immutable for life, so the identity gene stays constant even after resale or modification. The applicable safety rules, namely limits on flight area, altitude, and speed and the coordinates of no-fly zones, are cured into the system in encrypted form as hard constraints that the user cannot change or bypass. A unique key pair supports identity authentication, data encryption, and digital signature, with the private key never leaving the secure chip and the public key reported to the regulator, and key lifecycle events are recorded immutably in encrypted form to form a traceable chain.

The security gene is embedded across the full lifecycle. At the design stage, the security-gene architecture is built into the top-level hardware and software design. At production, dedicated encrypted-chip burning and a "one-machine-one-key" process complete native curing at the factory, and security-gene information is registered to a regulatory database. At sale, activation is bound to verification of purchaser qualification and to real-name registration, so every in-service UAV has a clearly responsible owner.

During operation, the security gene actively and intelligently avoids risk: when it detects a violating command, an incursion into a no-fly zone, an approach to a sensitive target, or an illegal modification, it independently triggers command refusal, limits manoeuvring, forces a return, or calls for a safe landing. It works like an instinct-like reflex and does not require any external instructions. At decommissioning, the security gene, the full-lifecycle traceability data, and the unique identity are retained permanently and cannot be deleted even after physical dismantling, which forecloses the hazards of illegal modification and secondary circulation of retired UAVs while leaving permanent, verifiable data for incident tracing and accountability. The cryptographic operations behind the gene use the Chinese commercial algorithms SM2, SM3, and SM4, with key generation, storage, use, and destruction governed by strict cryptographic discipline and with core data protected against physical, side-channel, and fault-injection attacks inside a hardware security module.

C. THE INTEGRATED SECURITY-CHIP ARCHITECTURE

In traditional UAV architectures the perception, communication, navigation, and control modules are relatively independent, and the safety function is an add-on bolted onto the system, an arrangement with low integration, blurred safety boundaries, and high response latency. As Figure 4 shows, the proposed sense–communicate–navigate–control integrated endogenous security-chip architecture uses system-on-chip technology to integrate a perception module, a communication module, a navigation module, a flight-control module, and a safety-supervision module, fusing core capability with supervisory capability under the principle of "function fusion, endogenous safety, performance optimisation."

The four functional modules each carry on-chip support. The perception module integrates visual, radar, and ultrasonic sensor interfaces with an on-chip neural-network accelerator for target recognition and obstacle detection. The communication module integrates multiple protocol stacks (4G/5G cellular, Wi-Fi, Bluetooth, and dedicated data links) with an encryption engine for end-to-end protection of commands and telemetry, a need underscored by comprehensive surveys of drone-communication security [29]. The navigation module integrates multi-constellation satellite reception and barometric altimetry to deliver high-precision position, velocity, and attitude. The flight-control module integrates the control processor and actuator interfaces with an on-chip safety-monitoring unit.

The most distinctive innovation is the safety supervision module, which is deeply integrated with the other four modules and is capable of implementing unique identity authentication, flight area control, real-time status reporting,

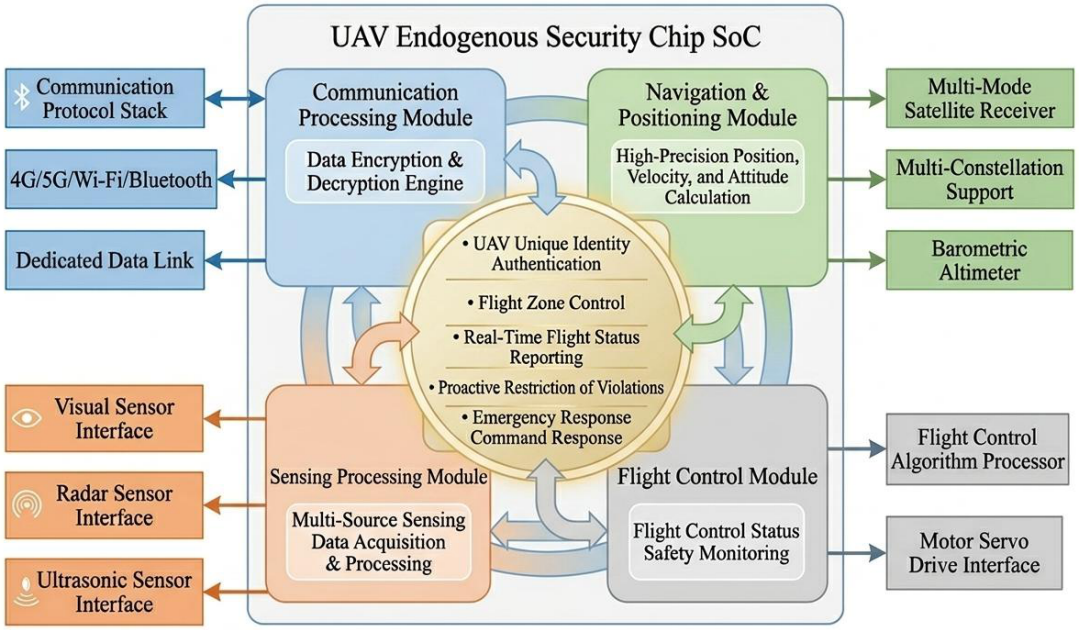

FIGURE 4. The sense–communicate–navigate–control integrated endogenous security-chip architecture.

proactive restriction of illegal behaviors, and emergency response. It uses a built-in key for two-way authentication with the supervision system to thwart control by counterfeit supervision ends. Under the protection of digital signatures, it reports status (position, altitude, speed, heading) at regular intervals. It compares the current location with the built-in electronic fence data in real time and triggers graded measures (alert, speed limit, height limit, forced return) when approaching or entering restricted airspace. It continuously monitors compliance with regulations, records and reports violations, and imposes restrictions simultaneously. In the event of communication interruption, navigation failure, or power failure, it autonomously initiates return, safe landing, or parachute descent according to the built-in strategy.

Performance is preserved through multi-core partitioning of safety and control tasks, hardware acceleration of cryptographic and inference workloads, dynamic voltage-and-frequency scaling for power efficiency, and redundancy with fault tolerance for critical modules.

V. LOW-ALTITUDE AIRSPACE ENVIRONMENT GOVERNANCE

A. STRUCTURAL CHARACTERISTICS OF URBAN LOW-ALTITUDE AIRSPACE

The airspace environment is the spatial carrier of flight and conditions safety directly. Urban low-altitude airspace is highly complex, dynamic, and heterogeneous, and the traditional management mode cannot accommodate the high-density, multi-scenario, fragmented operating pattern of UAVs; this has prompted proposals to treat low-altitude airspace as a strategic resource and to coordinate its development with surface and subsurface urban space. Vertically, the airspace is usually divided into three layers. The ultra-low layer (true height below 120 m) is the main activity region of micro, light, and small consumer UAVs and is marked by high flight density, complex scenarios, and acute risk sensitivity. The low-to-medium layer (120–300 m) is the main region of logistics and inspection UAVs, with comparatively regulated activity. The medium-to-high layer (300–1000 m) is the region of medium and large UAVs and of the eVTOL aircraft envisaged for urban air mobility, with the strongest demands on safety and order.

The layers differ markedly in risk profile, control requirement, and technical condition. The ultra-low layer is most closely interwoven with ground activity and places the highest demands on obstacle avoidance, noise control, and privacy protection, whereas the low-to-medium layer carries greater conflict risk with manned aircraft and places higher demands on coordination, communication assurance, and emergency handling.

Horizontally, the Interim Regulations on the Administration of Unmanned Aircraft Flight divide urban low-altitude airspace into controlled airspace and suitable-for-flight airspace. Controlled airspace includes the airspace above 120 m, air-prohibited zones and their surroundings, military ultra-low-altitude flight airspace, and the airspace above airports, borders, military zones, important military and public infrastructure, facilities needing special electromagnetic protection, and major commemorative sites; flight there requires approval from the air-traffic-management au-

thority. Suitable-for-flight airspace is the complement, where micro UAVs may fly below 50 m true height and light and small UAVs below 120 m without filing a flight application, and the regulations also allow temporary additions to controlled airspace under special circumstances.

Zone delineation should balance safety, economic efficiency, and technical feasibility, with boundaries clear enough for onboard systems and operators to recognise and obey, and with the capacity for temporary dynamic adjustment to support major-event security and contingency disposal. The physical, meteorological, and electromagnetic complexity of the city, including urban canyons, microscale turbulence and gusts, the heat-island effect, dense electromagnetic-radiation sources, and congested control bands, together with the threat of deliberate navigation spoofing and link suppression, requires governance to adopt a refined, risk-graded strategy keyed to the density of sensitive targets, the distribution of population, and the differentiated risk level of each scenario.

B. RULE-BASED CONSTRAINT OF AIRSPACE OPERATIONS

The main purpose of rule-based constraints is to convert the legal requirements, safety standards, and operational norms of airspace management into digital rules that onboard systems and regulatory platforms can understand and carry out. This way, airspace rules are built in from the start and enforced automatically. The advantages are clear: enforcement becomes more predictable and consistent, which helps prevent hazards caused by human misreading or omissions; automatic enforcement and real-time checks cut down on manual effort and reduce response times; updating and managing versions is much easier; and autonomous flights operate within a measurable safety boundary that enables higher levels of automation.

As Figure 5 shows, automatic enforcement depends on encoding the rules in a machine-processable way. This can be done with a dedicated rule-expression language or by using an existing rule-engine technology, while weighing human readability against machine usability. The encoding specifications should spell out the rule formats, fields, value ranges, classification, version control, and dependency relationships. A digital distribution mechanism then pushes encoded rules to onboard systems and regulatory platforms, with support for incremental update, differential synchronisation, and rollback to keep them consistent and current, while rule-execution engines embedded in both onboard systems and platforms parse and run the rules in real time with high performance and low latency.

Because airspace rules must be adjusted dynamically for major-event security, key-target protection, and contingency disposal, the system must support rapid release of temporary rules, each with a clear validity period, scope, control requirement, and lifting condition, together with automatic activation and expiry, conflict resolution between temporary and routine rules (with temporary rules generally taking precedence), and continuous monitoring of execution to detect and correct deviations. This digitally enforced approach is the airspace-environment counterpart of the UTM and U-space principle that only authenticated UAVs operate in the airspace and that all constraints, in the air and on the ground, are knowable to the operator and the system.

VI. MANAGEMENT-ELEMENT GOVERNANCE

A. UAV FULL-LIFECYCLE MANAGEMENT

The management element is the institutional guarantee and operating mechanism of low-altitude safety governance, the adhesive that binds the human, machine, and environment elements into coordinated operation. Effective governance needs a management system that covers all elements, the full chain, and the whole lifecycle, with deep integration of institutions and technical systems. UAV full-lifecycle management governs the entire process from design, production, and sale through use to decommissioning, ensuring that every stage meets safety requirements and forming a complete safety chain that supports full-process traceability of responsibility, full-process recording of safety information, and full-process implementation of safety requirements.

As Figure 6 shows, the requirements differ by stage. At design, the brief specifies safety requirements such as applicable standards, mandatory safety functions, and acceptable risk levels, and an intrinsic-safety architecture with redundancy, fault tolerance, and testability is adopted, supported by systematic hazard identification, risk analysis, and safety assessment. At production, a quality-management system controls raw-material procurement, component machining, assembly, and inspection; the security gene (unique identity, encryption key, and safety rules) is written using dedicated equipment and processes; and every unit undergoes full functional, performance, and safety testing before delivery. At sale, dealers keep sales ledgers recording the destination of each unit, disclose safety information to users, and implement real-name registration together with an activation-control mechanism that requires real-name registration, qualification verification, and safety training, linked in real time to the regulatory system, before flight functions are unlocked.

The use stage is the longest and most complex. It calls for operational safety-management systems covering pre-flight inspection, in-flight monitoring, and post-flight review, with stricter regimes for commercial operation, real-time monitoring through flight-service platforms, and maintenance that uses original or certified parts for safety-critical components. The decommissioning stage is easily overlooked but matters: clear retirement criteria are defined, user privacy data are irrecoverably erased while the identity and traceability records of the security gene are retained permanently, and core components are specially treated to prevent illegal salvage and reuse.

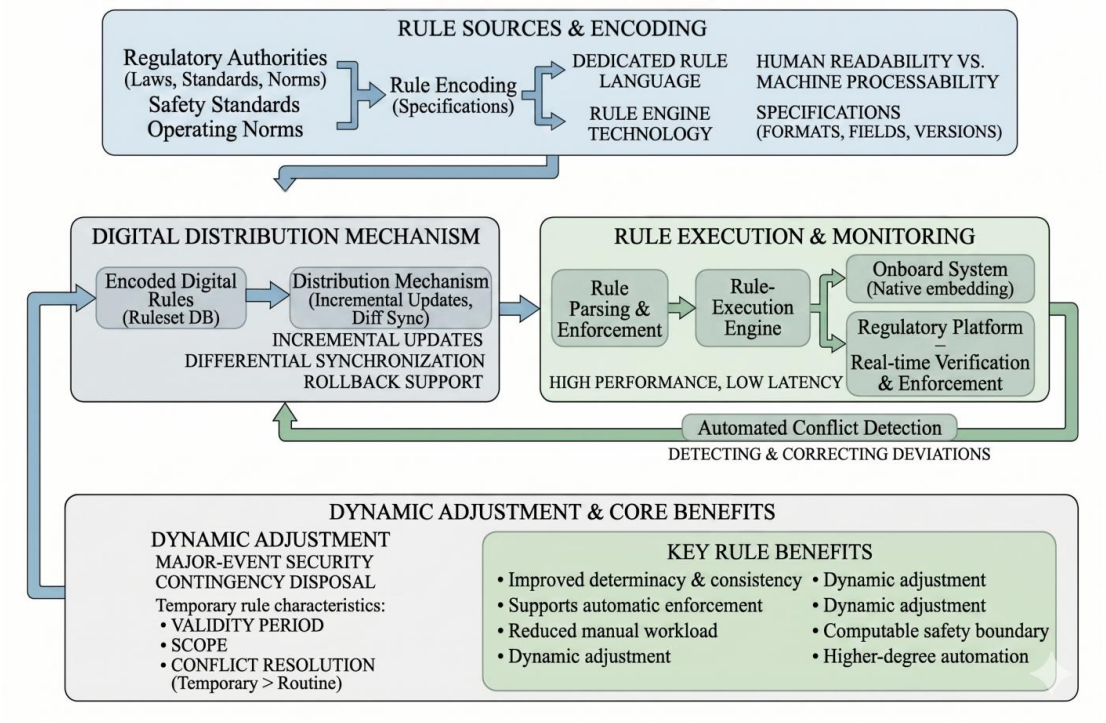

FIGURE 5. Rule-based constraint of airspace operations.

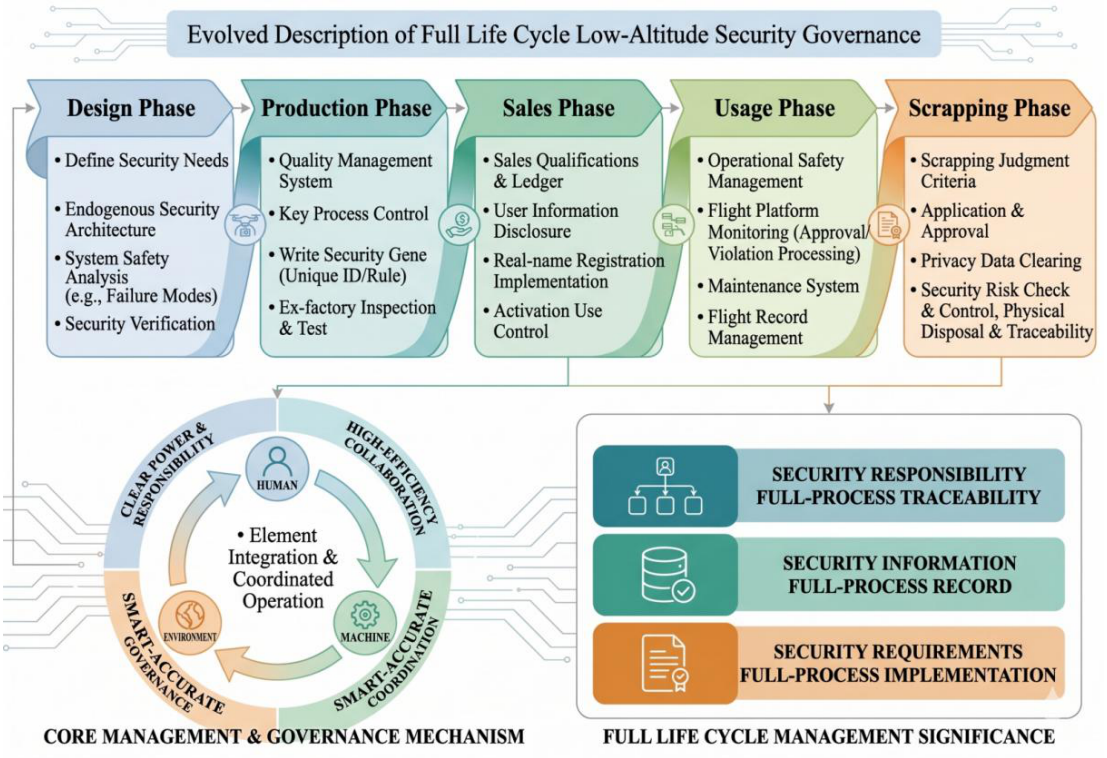

FIGURE 6. The UAV full-lifecycle safety-management mechanism.

B. A CONSORTIUM-BLOCKCHAIN LIFECYCLE RECORD SYSTEM

Centralised storage of UAV data carries single-point-of-failure risk, data-tampering risk, and cross-departmental data barriers. We therefore propose a blockchain-based UAV full-lifecycle record system (UAV-BCLR) with a consortium-blockchain architecture, designed to provide trustworthy,

tamper-resistant, multi-party-shared records from design and production through to decommissioning and deregistration. A blockchain supplies an append-only, tamper-evident distributed ledger that removes reliance on a single trusted custodian [30], and its application to UAV systems, for identity, data integrity, and secure coordination, has become an active research direction [31].

The UAV-BCLR consortium chain has five node classes: regulatory nodes (air-traffic management, civil aviation, public security, and industry and information technology), manufacturer nodes, operator nodes, maintenance-organisation nodes, and insurance-organisation nodes. It uses the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, which provides state-machine replication that tolerates Byzantine faults in asynchronous environments such as the Internet [32] and suits permissioned settings with a known, modest set of validating nodes. Each UAV corresponds to one immutable on-chain identity whose records span product-conformity certification, operator-binding changes, flight-mission execution, maintenance, penalty records, and decommissioning certificates; smart contracts perform compliance checks automatically, and violation records are broadcast in real time to all regulatory nodes.

On-chain triggering conditions and access permissions are differentiated by lifecycle stage. Design-production records, for example, are triggered on certification approval and readable by regulators and the manufacturer, whereas sales-registration records are triggered on completion of real-name registration and readable by all nodes, which balances transparency against confidentiality. This design is consistent with the wider Internet-of-Drones security literature, which identifies trustworthy identity management and tamper-resistant record-keeping as foundational requirements.

C. COUNTER-UAS EQUIPMENT GOVERNANCE AND MANAGEMENT–TECHNOLOGY SYNERGY

Counter-UAS equipment is the technical means of responding to violating UAVs, yet the equipment itself can introduce risk, since mismanagement may lead to abuse, misuse, and secondary harm. Its full-lifecycle management therefore carries special importance, with the dual aim of remaining effective against threats while preventing abuse, interference with legitimate flight, and harm to the surrounding electromagnetic environment and to people, an aim consistent with the safety considerations stressed across the counter-UAS state of the art. Design and production must meet strict technical and electromagnetic-compatibility standards, with effective range, coverage, and response time specified and interference to surrounding electronics limited; radio-suppression devices must control transmit power, and physical-interception devices must keep impact points controllable.

Sale and use should be governed by a strict licensing regime that confines use to military, public-security, national-security, and critical-infrastructure-management organisations holding statutory enforcement or safety-management responsibilities, with sales ledgers reported to regulators and use confined to cases in which a violating UAV has been detected and prior ground-disposal means have failed, following the principle of proportionality. A digital management system assigns each device a unique identity and equipment file, registers deployment (location, coverage, and operating unit) with regulators, records every use (time, location, target, disposal mode, and result) in real time for traceability and effectiveness evaluation, and monitors operating status.

One of the prominent issues in current governance is the disconnection between management and technology. Regulations, standards and processes often remain on paper, while the technical system, although equipped with monitoring and handling capabilities, lacks rule guidance. To achieve collaboration, it is necessary to convert management systems into executable rules, processes and permission models for the technical system. The no-fly and permitted flight zones should be transformed into electronic fence data, altitude restrictions into parameter constraints, the qualifications of control personnel into identity verification rules, and flight approval, violation handling and emergency response into automatically executable process engines and role-based permission models. The operation, data and approval permissions should be clearly defined.

Once that is in place, technical systems don't just execute the rules. They also enable management decision-making: they use the perception network to build a complete situational picture, use AI analysis to uncover hidden risks, and provide decision-support tools that recommend disposal plans and resource allocation while assessing how effective the measures are — so the system can support continuous improvement. A management–technology linkage mechanism finally closes the loop in real time. A submitted flight plan triggers automatic compliance and conflict checks whose results feed an approval decision synchronised to onboard systems and the service platform. A detected violation generates an alert that, once confirmed, dispatches disposal commands whose process and result are returned in real time. A contingency triggers automatic event identification, impact assessment, and scheme recommendation, with confirmed emergency commands dispatched and resources scheduled automatically. And multi-departmental joint enforcement is supported by a unified situational picture and communication platform with unified command dispatch and real-time recording.

VII. CONCLUSION

This paper has developed a source-oriented safety governance framework for urban UAVs, organised around the coordinated treatment of the human, machine, environment, and management elements. At the level of element composition, it has analysed the behavioural-subject character of the human element, the technical-carrier attributes of the machine element, the spatial-field function of the en-

vironment element, and the institutional-guarantee role of the management element, and it has clarified their interrelated, dynamically coupled relationship. For human-factor governance it has built a full-cycle admission–assessment–supervision–exit system anchored by a four-layer intelligent risk-assessment model with attention-based dynamic weighting and LSTM trend prediction. For intrinsic safety it has proposed the shift from embedded to endogenous protection, realised through a security-gene embedding mechanism and an integrated sense–communicate–navigate–control security chip. For environment governance it has analysed the layered and zoned structure of urban low-altitude airspace and proposed a digital, rule-based constraint mechanism. For management governance it has established UAV and counter-UAS full-lifecycle management, supported by a consortium-blockchain record system and a management–technology synergy mechanism.

Taken together, the framework embodies the shift from after-the-fact disposal to source prevention, identifying, neutralising, and forestalling low-altitude safety risk at its logical origin through whole-lifecycle, whole-process proactive control of the four elements. Future work should focus on empirical calibration of the human-factor model's indicator weights and fusion coefficients on operational data, on standardising the interfaces of new low-altitude infrastructure to dissolve information islands, and on field validation of the integrated security chip and of UAV-BCLR consensus performance at city scale.

CONFLICTING INTERESTS

The authors declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

ACKNOWLEDGMENT

This work was supported by Beijing Natural Science Foundation (L232003), General Project of Beijing Municipal Social Science Foundation (24JCC095), Public Security Behavioral Science and Engineering Action Project of People's Public Security University of China (2022KXGCKJ07).

REFERENCES

[1] P. Kopardekar, J. Rios, T. Prevot, M. Johnson, J. Jung, and J. E. Robinson, "Unmanned aircraft system traffic management (UTM) concept of operations," in *Proc. 16th AIAA Aviation Technology, Integration, and Operations Conf. (ATIO)*, Washington, DC, USA, Jun. 2016, paper AIAA 2016-3292.

[2] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, Art. no. 7, pp. 1–25, Nov. 2016.

[3] C. Barrado, M. Boyero, L. Brucculeri, G. Ferrara, A. Hately, P. Hullah, D. Martin-Marrero, E. Pastor, A. P. Rushton, and A. Volkert, "U-space concept of operations: A key enabler for opening airspace to emerging low-altitude operations," *Aerospace*, vol. 7, no. 3, Art. no. 24, Mar. 2020.

[4] A. P. Cohen, S. A. Shaheen, and E. M. Farrar, "Urban air mobility: History, ecosystem, market potential, and challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 6074–6087, Sep. 2021.

[5] S. S. Ahmed, G. Fountas, V. Lurkin, P. C. Anastasopoulos, Y. Zhang, M. Bierlaire, and F. Mannering, "The state of urban air mobility research: An assessment of challenges and opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 2, pp. 1375–1394, Feb. 2025.

[6] H. Huang, J. Su, and F.-Y. Wang, "The potential of low-altitude airspace: The future of urban air transportation," *IEEE Trans. Intell. Veh.*, vol. 9, no. 8, pp. 5250–5254, Aug. 2024.

[7] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of Drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[8] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of Drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[9] M. A. Khan, H. Menouar, A. Eldeeb, A. Abu-Dayya, and F. D. Salim, "On the detection of unauthorized drones—Techniques and future perspectives: A review," *IEEE Sensors J.*, vol. 22, no. 12, pp. 11439–11455, Jun. 2022.

[10] M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Gener. Comput. Syst.*, vol. 100, pp. 86–97, 2019.

[11] Z. Shi, X. Chang, C. Yang, Z. Wu, and J. Wu, "An acoustic-based surveillance system for amateur drones detection and localization," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2731–2739, Mar. 2020.

[12] J. Wang, Y. Liu, and H. Song, "Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–29, Mar. 2021.

[13] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, Art. no. 102324, Feb. 2021.

[14] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, "A review of counter-UAS technologies for cooperative defensive teams of drones," *Drones*, vol. 6, no. 3, Art. no. 65, 2022.

[15] N. G. Leveson, "A new accident model for engineering safer systems," *Safety Sci.*, vol. 42, no. 4, pp. 237–270, Apr. 2004.

[16] B. Fan, Y. Li, and R. Zhang, "Initial analysis of low-altitude internet of intelligences (IOI) and the applications of unmanned aerial vehicle industry," *Progress in Geography*, vol. 40, no. 9, pp. 1441–1450, 2021 (in Chinese).

[17] X. Liao, Y. Huang, and C. Xu, "Views on the study of low-altitude airspace resources for UAV applications," *Acta Geographica Sinica*, vol. 76, no. 11, pp. 2607–2620, 2021 (in Chinese).

[18] J. Liu, X. Su, and Z. Shen, "Exploring the collaborative development model of urban low-altitude airspace and surface–subsurface spaces oriented by UAV-based traffic governance," *Urban Planning International*, early access, 2024 (in Chinese).

[19] State Council and Central Military Commission of the People's Republic of China, *Interim Regulations on the Administration of Unmanned Aircraft Flight*, 2023 (effective 1 Jan. 2024).

[20] H. W. Heinrich, *Industrial Accident Prevention: A Scientific Approach*. New York, NY, USA: McGraw-Hill, 1931.

[21] X. Feng, M. Ouyang, X. Liu, L. Lu, Y. Xia, and X. He, "Thermal runaway mechanism of lithium ion battery for electric vehicles: A review," *Energy Storage Mater.*, vol. 10, pp. 246–267, 2018.

[22] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[23] Y. Dang, C. Benzaïd, B. Yang, T. Taleb, and Y. Shen, "Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25068–25085, Dec. 2022.

[24] J. McCoy, A. Rawal, D. B. Rawat, and B. M. Sadler, "Ensemble deep learning for sustainable multimodal UAV classification," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15425–15434, Dec. 2023.

[25] A. Yasmeen and O. Daescu, "Recent research progress on ground-to-air vision-based anti-UAV detection and tracking methodologies: A review," *Drones*, vol. 9, no. 1, Art. no. 18, 2025.

[26] J. Reason, *Human Error*. Cambridge, U.K.: Cambridge Univ. Press, 1990.

[27] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in *Advances in Neural Information Processing Systems 30 (NeurIPS)*, pp. 5998–6008, 2017.

[28] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.

[29] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2802–2832, 2021.

[30] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[31] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, Art. no. 100249, 2020.

[32] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI '99)*, New Orleans, LA, USA, pp. 173–186, 1999.