Research on the Construction of a Low-Altitude Security System for Major Event Security

Jianchun Li*

The 53rd Research Institute of China Electronics Technology Group Corporation, Tianjin, 30000, China
**Corresponding author: 18822626886@163.com*

Abstract: *With the opening of low-altitude airspace and the proliferation of drone technology, low-altitude security has become a critical component of the security system for major events. Addressing the diversified and dynamic characteristics of contemporary low-altitude threats, this paper systematically constructs a low-altitude security system for major event security. By defining the conceptual connotation and layered architecture of the low-altitude security system, it proposes a core model based on Cyber-Physical Systems and system resilience theory. The paper further analyzes the classification characteristics and behavioral patterns of multi-source, heterogeneous low-altitude threats, establishing a dynamic risk assessment framework that incorporates spatiotemporal constraints. Building upon this foundation, it designs a technical pathway for collaborative perception and intelligent response via a multi-dimensional sensor network, enabling closed-loop management from threat detection to response decision-making. The research demonstrates that this system can significantly enhance the real-time perception capability, risk assessment accuracy, and response efficiency regarding low-altitude threats, providing theoretical support and technical solutions for low-altitude security during major events.*

Keywords: *low-altitude security; security system; threat assessment; collaborative perception; intelligent response; system resilience*

Introduction

Low-altitude security has emerged as a critical new domain within the security framework for major events. The threats it faces are characterized by high suddenness, low technical barriers, and significant difficulty in prevention and control, making traditional single-technology or decentralized management models inadequate for effectively addressing systemic risks. The rapid development and widespread application of low-altityde aircraft technology have led to increasingly complex forms of low-altitude threats, such as non-cooperative intrusions, malicious detection, and electromagnetic interference, posing severe challenges to the airspace security of major events. Existing research predominantly focuses on breakthroughs in singular technological aspects and lacks an integrated, systematic design encompassing the entire chain from architectural framework to risk assessment and, finally, to response and disposal. Consequently, constructing a low-altitude security system that integrates the functions of perception, assessment, decision-making, and response holds significant theoretical value and practical urgency. This paper conducts systematic research ranging from system architecture design and threat modeling assessment to technical implementation pathways, aiming to establish a scientific and comprehensive methodology for constructing a low-altitude security system. It seeks to provide a systematic solution for the safety and security management of low-altitude airspace during major events.

1. Core Architecture and Theoretical Foundation of the Low-Altitude Security System

1.1 Conceptual Connotation and Constituent Elements of the Low-Altitude Security System

The low-altitude security system is a complex adaptive system designed to safeguard specific airspace. Its core connotation is reflected in the deep collaboration and closed-loop control of system components, enabling the continuous monitoring, accurate assessment, and graded intervention of dynamic low-altitude targets. This system differs fundamentally from traditional airspace management

systems in the diversity of threat forms it faces, the real-time requirements for response decisions, and the highly adversarial nature of its operational environment. Regarding its composition, the system can be analyzed from two dimensions: the static infrastructure and the dynamic interaction mechanisms.

The static infrastructure forms the material foundation of the system. It includes multi-source sensor nodes deployed on the ground, rooftops, and aerial platforms; data link networks supporting high-bandwidth, low-latency transmission; distributed processing hubs with high-performance computing capabilities; graded countermeasure units ranging from soft-kill to hard-kill options; and standardized protocol stacks ensuring system interoperability.

These fundamental components form an organic whole through dynamic interaction mechanisms. The dynamic interactions primarily manifest as a closed loop comprised of perception data flows based on a unified spatiotemporal reference, control command flows generated according to threat assessment results, and real-time feedback information flows reflecting the effects of countermeasures [1]. Through online learning and parameter self-adaptation mechanisms, this closed-loop system can generate coordinated responses to environmental changes and threat evolution. The overall efficacy of the system depends not only on the performance metrics of individual components but, more importantly, stems from the information sharing and functional collaboration achieved between components via standardized interfaces. This architectural characteristic endows the system with the resilience to cope with emergent threats and complex scenarios.

1.2 Construction of a Hierarchical Control-Based Architectural Model for the System

To address the complexity challenges in designing the low-altitude security system, this section proposes an architectural model based on the concept of hierarchical control. This model vertically divides the system into five logical layers through functional decoupling and hierarchical encapsulation, with standardized interfaces facilitating data exchange and command transmission between the layers. The Physical Perception Layer, serving as the system's boundary for interaction with the environment, integrates both active and passive detection equipment. This includes phased array radars, software-defined radio monitoring systems, infrared and visible light fused imaging devices, and acoustic arrays, achieving wide-area coverage and feature collection of low-altitude targets. The Network Transmission Layer constructs the information highway for the system. It employs time-sensitive networking and anti-jamming communication technologies to ensure the reliable transmission and timing guarantees of perception data and control commands within complex electromagnetic environments.

The Data Fusion Layer is responsible for extracting value from multi-source information. Utilizing algorithms for spatiotemporal registration, feature extraction, and correlation matching, it transforms raw heterogeneous observation data into a tactical situation map with a unified format. This layer employs algorithms such as deep learning and Kalman filtering to effectively enhance the detection probability and tracking accuracy of low, slow, and small (LSS) targets. The Intelligent Decision-Making Layer is the core cognitive unit of the system. Based on the fused situational information, it uses threat assessment models, behavior prediction algorithms, and decision theory to generate optimal response strategies for different threat levels. The Collaborative Response Layer then translates abstract decisions into concrete actions. By uniformly scheduling countermeasure resources such as navigation spoofing, electromagnetic suppression, and kinetic interception, it achieves a precise response to non-cooperative targets. This layered architecture ensures the modular development of system functions and the smooth evolution of technologies [2].

1.3 Key Theoretical Support and Methodology for System Construction

The construction of the low-altitude security system relies on the interdisciplinary integration of theories and the guidance of systematic engineering methodologies. Cyber-Physical Systems (CPS) theory provides the foundational framework for the system. This theory emphasizes the deep integration of computational units and physical processes, ensuring that decision commands from the information space can accurately drive the perception and execution units in the physical world through the establishment of precise digital models, thereby achieving cross-domain collaboration. System resilience theory expands upon traditional reliability concepts. It guides the system design to shift from solely pursuing robustness towards focusing on function maintenance and rapid recovery under conditions of attack, component failure, or performance degradation, specifically realized through mechanisms such as heterogeneous redundancy, functional reconfiguration, and online learning.

Game theory provides the mathematical tools for analyzing attack-defense confrontational behaviors. By constructing non-cooperative game models, it enables the prediction of potential adversary behavior patterns and the optimization of dynamic allocation of defense resources and response strategies. At the methodological level, Model-Based Systems Engineering (MBSE) is established as the dominant method for system construction. This method employs formalized system models throughout the entire lifecycle, encompassing requirements analysis, functional definition, logical design, and physical implementation, ensuring consistency, completeness, and traceability across all design stages. Digital twin technology, as a key practice of this method, supports the verification and optimization of the system architecture and the predictive maintenance of its operational status by constructing a virtual replica synchronized with the physical system, significantly enhancing the efficiency and quality of the systems engineering process.

2. Identification and Dynamic Risk Assessment of Low-Altitude Multi-Source Heterogeneous Threats

2.1 Classification and Behavioral Characteristic Analysis of Low-Altitude Threat Sources

The accurate identification and behavioral modeling of low-altitude threat sources form the cornerstone of implementing active defense. Based on the physical attributes, behavioral intent, and tactical objectives of threat carriers, a multi-dimensional, hierarchical threat classification system can be constructed. This system primarily distinguishes between platform types, covering Unmanned Aerial Systems (UAS) ranging from micro, consumer-grade to industrial custom-grade, as well as other low, slow, and small (LSS) aircraft such as ultralight aircraft and motorized gliders. On this basis, a secondary classification is required according to their mission behaviors, primarily categorized into four types: reconnaissance and surveillance, territorial intrusion, material delivery, and electromagnetic interference. The core behavioral characteristics of reconnaissance and surveillance threats manifest as regular close-range reconnaissance of sensitive areas, multi-angle hovering observation, and the use of data links employing frequency hopping and low probability of intercept technologies for information transmission. Territorial intrusion threats focus on breaching airspace boundaries. Their behavioral patterns typically employ tactics such as terrain-following, low-altitude silent penetration, or coordinated swarm assaults, often accompanied by active countermeasures like radio silence and false identity broadcasts [3].

In-depth analysis of threat behavioral characteristics requires further integration of their technical implementation mechanisms. Platforms associated with delivery threats often exhibit specific flight performance, such as high payload capacity, stable hovering accuracy, and precise takeoff/landing control. Their flight path planning frequently demonstrates rapid maneuver patterns transitioning from the periphery to a point above the target. The essence of jamming threat behavior lies in confrontation within the electromagnetic spectrum domain. Its typical characteristics include the presence of high-power barrage noise, structured spoofing signals, or precise protocol-level injection attacks in specific navigation or communication frequency bands, leading to perception blindness or decision-making disruption within the defense system. These quantified behavioral characteristic parameters constitute the key input variables for subsequent threat intent identification and risk assessment models, enabling the transition of threat prediction from qualitative judgment to quantitative analysis.

2.2 Dynamic Risk Assessment Framework Integrating Spatiotemporal Constraints

Traditional static risk assessment models struggle to adapt to the rapidly evolving low-altitude situations in major event security scenarios, making it essential to construct a dynamic risk assessment framework that integrates spatiotemporal constraints. The theoretical foundation of this framework lies in redefining risk as a dynamic function of four elements: threat, vulnerability, consequence, and spatiotemporal context. Its innovation is reflected in the introduction of a spatiotemporal grid-based modeling concept, which discretizes the entire security airspace and its adjacent areas into basic units with unified spatiotemporal identifiers. The risk value of each unit is an emergent result of the combined effect of instantaneous threat attributes, geographical context, and time sensitivity within that unit.

The operation of this framework relies on a multi-tiered computational engine. The bottom layer consists of real-time situational awareness data streams, providing the identity confidence,

three-dimensional position, velocity vector, and signal characteristics of threat targets. The middle layer is the context computation layer, which incorporates static and dynamic geographical constraints—such as critical infrastructure coordinates, building occlusion effects, and real-time population heat maps—via Geographic Information System (GIS) embedding, while also integrating the event schedule timeline to define security criticality levels for different time periods. The top layer is the risk fusion layer, which employs algorithms such as Bayesian networks, fuzzy logic, or deep belief networks to dynamically compute and aggregate the uncertainty of each factor, ultimately outputting a high-resolution, refreshable panoramic view of the dynamic risk situation. This map can not only visually display the current spatial distribution of risks and hotspot areas but also, through short-term prediction models, simulate the evolution trends of risks within future time windows, thereby achieving a paradigm shift from passive response to proactive early warning.

2.3 Analysis of Vulnerability Propagation Paths Based on Threat Intelligence

The defensive efficacy of the low-altitude security system is a function determined by both external threats and endogenous vulnerabilities. Systematically identifying and blocking the propagation paths through which vulnerabilities can be exploited is crucial for enhancing system resilience. Here, vulnerability is defined as a design flaw or performance boundary within the system's technical architecture, information flow, or decision-making logic that can be exploited by a threat. Its manifestations are diverse, encompassing detection blind spots and multipath effects of sensor networks in complex urban canyon environments; the degradation of correlation algorithm confidence in data fusion centers when processing heterogeneous, asynchronous information; the sharp increase in interruption probability of wireless communication links in adversarial electromagnetic environments; and the lack of elastic response strategies in command-and-control rule bases for unknown attack patterns [4].

The threat intelligence-based propagation path analysis aims to formally delineate the attack chain. This method uses attack graphs or fault trees as modeling tools, treating identified system vulnerabilities as nodes and the Tactics, Techniques, and Procedures (TTPs) of threats as edges, to construct a set of all possible paths from the initial point of infiltration to the final attack objective. Each path represents a causal chain wherein a threat progressively achieves its attack goal by exploiting a series of vulnerabilities. By conducting a quantitative analysis of these paths based on probabilistic risk assessment—such as calculating the product of the attack success probability and potential loss for each path—the most critical attack paths within the system can be identified. This analysis elevates system defense from patching individual vulnerabilities to the strategic management of the overall attack surface. It guides the prioritization of defense resources for deploying deceptive nodes, adding heterogeneous redundant links, or formulating dynamic policy switching mechanisms, thereby most effectively severing the propagation chains of high-risk threats and fundamentally optimizing the overall security resilience of the system.

3. Technical Pathways for Collaborative Perception and Intelligent Response in the Low-Altitude Security System

3.1 Collaborative Detection and Data Fusion of Multi-Dimensional Sensor Networks

The perceptual capability of the low-altitude security system is founded upon the collaborative operation of a heterogeneous multi-source sensor network. This network establishes all-weather, all-airspace seamless surveillance capabilities through spatially distributed, spectrally covered, and functionally complementary sensor nodes. Its technical core lies in resolving the disparities in data format, spatiotemporal reference, and observation accuracy among different sensor types, thereby achieving the transformation from raw data to unified situational information. Radar systems provide precise target range and velocity vectors; radio frequency spectrum monitoring equipment captures the communication and navigation signal characteristics of targets; electro-optical sensors contribute high-resolution visual feature information; and acoustic arrays can be used for auxiliary localization and classification. The collaborative fusion of these heterogeneous data sources forms the basis for low-altitude target detection and identification.

The data fusion process employs a multi-level processing architecture. At the data-level fusion stage, spatiotemporal references are aligned to enable the direct correlation and complementation of multi-source observation data for the same target. At the feature-level fusion stage, deep learning

models are utilized to extract abstract features from the data of each sensor, and feature concatenation and joint classification are performed in a high-dimensional space, significantly enhancing the detection probability and identification accuracy for low, slow, and small (LSS) targets. At the decision-level fusion stage, methods such as D-S evidence theory or Bayesian inference are applied to synthesize the local judgment results from independent perception channels, generating a globally consistent target identification and threat level assessment. This multi-level fusion mechanism effectively reduces the false alarm and missed detection risks associated with any single sensor, forming a stereoscopic, high-confidence awareness of the low-altitude environment [5].

3.2 Intelligent Decision-Making and Disposal Strategy Generation for Non-Cooperative Targets

Confronted with the complex adversarial behaviors of non-cooperative targets, the low-altitude security system requires autonomous and efficient intelligent decision-making capabilities. The decision-making process takes the real-time fused situation as input and comprehensively considers multiple constraints, including the target's threat level, airspace security boundaries, and the status of disposal resources. Its core technology is a hybrid decision-making architecture that combines rule-based and model-based approaches. The rule base defines standardized response procedures for known threat patterns, while predictive models evaluate the potential effects and cascading consequences of different disposal strategies through online simulation and deduction.

The generation of intelligent disposal strategies follows a principle of graded escalation. Based on the threat assessment results, the system automatically produces a graduated response plan ranging from warning and expulsion to hard-kill destruction. For low-threat targets, non-kinetic means such as radio warnings and navigation signal jamming are prioritized. For medium-to-high threat targets, measures can be escalated to coercive actions such as protocol-level takeover, GNSS spoofing, or net-capture interception. Kinetic strike options like laser interception are initiated only as a last resort in extreme circumstances. Strategy generation algorithms, such as online reinforcement learning or evolutionary computation, can optimize disposal parameters and resource scheduling schemes in real-time according to the dynamic changes in the adversarial environment. This ensures the formation of an optimal response strategy within the shortest possible time, achieving extreme compression of the OODA (Observe-Orient-Decide-Act) cycle.

3.3 Disposal Efficacy Evaluation and System Resilience Recovery Mechanism

The continued effectiveness of the low-altitude security system relies on the precise evaluation of disposal action efficacy and the system's resilience recovery capability. Efficacy evaluation is established upon a multi-dimensional quantitative indicator system, encompassing timeliness indicators, resource utility indicators, and tactical effect indicators. Timeliness indicators include the decision-making cycle from target detection to disposal completion, as well as system response latency. Resource utility indicators assess the consumption and cost-effectiveness of various countermeasure measures. Tactical effect indicators measure the degree of threat containment achieved by disposal actions and their collateral effects. By constructing a digital twin environment, various disposal plans can be simulated, tested, and their efficacy predicted both before and after operations.

The system resilience recovery mechanism is designed to ensure that the system can maintain its core security functions and rapidly return to normal operation even when subjected to saturation attacks, component failures, or performance degradation [6]. This mechanism comprises three levels: Passive resilience provides the system with inherent fault tolerance through equipment redundancy, multi-path communication, and functional backups. Active resilience achieves function maintenance and performance optimization under impaired conditions through resource reconfiguration, task reassignment, and strategy adaptation. Adaptive resilience endows the system with the ability to learn from confrontations; by analyzing the correlation between attack patterns and disposal outcomes, it dynamically updates the threat knowledge base and optimizes decision-making models, enabling self-evolution and capability enhancement of the system. This multi-layered resilience design allows the low-altitude security system to calmly cope with complex and volatile adversarial environments, ensuring sustained and stable security effectiveness.

Conclusion

This paper systematically constructs a low-altitude security system for major event security. It

proposes a core architectural model based on hierarchical control, establishes a multi-dimensional threat classification system and dynamic risk assessment methodology, and designs a complete technical pathway from collaborative perception to intelligent response. Research demonstrates that this system, through the deep fusion of multi-source heterogeneous data, the accurate prediction of threat behaviors, and the automatic generation of graded response strategies, enables full-process management of low-altitude security risks. The system architecture possesses strong scalability and adaptability, allowing for dynamic adjustments according to different application scenarios and threat evolution.

Future research will focus on the deepened application of intelligent algorithms in the early identification of threat intent, particularly the construction of abnormal behavior detection models based on few-shot learning. It will explore resilience enhancement mechanisms for cross-domain collaboration, investigating functional reconfiguration and resource scheduling optimization for heterogeneous systems under partial failure conditions. Efforts will also advance the real-time interaction capability between digital twin technology and physical systems, building a simulation verification platform with predictive maintenance functions. Concurrently, attention must be paid to the deployment architecture of intelligent edge computing in distributed perception nodes, and multi-agent decision-making mechanisms for countering swarm threats. These research directions will propel the low-altitude security system towards a capability leap—from passive response to active early warning, and from static defense to dynamic adaptation—laying a theoretical foundation for constructing a next-generation low-altitude security system with continuous evolution capabilities.

References

[1] Zhang Jinran. "Wu Qihui: Constructing a Spectrum Security System to Safeguard the Development of the Low-Altitude Economy." China Radio. .09 (2025): 29-31.

[2] Zhang Xiao, Xie Xiaoqin, and Wang Zhan. "Standardization Path for the UAV Inspection and Testing System from the Perspective of Low-Altitude Security." Quality and Certification. .08 (2025): 37-39.

[3] Zhang Qin, and Zhu Dengxuan. "Research on the Practical Dimensions of Low-Altitude Economic Security Risks and Governance—A Dynamic Analysis Based on Technology Risk Derivation." Urban Development Studies 32.06 (2025): 1-8.

[4] Wang Lili. "Thoughts and Explorations on the Construction of a Low-Altitude Security System." Robot Industry. .03 (2025): 52-56.

[5] Wang Hongtao, et al. "Discussion on the Construction of a Standardization System for Low-Altitude Economic Security Risk Prevention." Quality, Safety and Inspection & Testing 35.02 (2025): 37-40+48.

[6] Feng Haiming, Yu Wenshuang, and Wang Ping. "Analysis of the Architecture and Scenario Application of a Low-Altitude Security Supervision Platform." China Security & Protection. .04 (2025): 88-91.