Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P3334-cd

Research on Resilience and Security of Cluster Unmanned Systems Based on Backup Complementary Strategy

Lin Shen

China Academy of Aerospace Standardization and Product Assurance, Beijing China, Shenlin708@139.com

ZhaoJun Yang

China Aerospace Science and Technology Corporation, Beijing China, liuyub2@163.com

TianLong Han

China Academy of Aerospace Standardization and Product Assurance, Beijing China, longlong0410@163.com

HaiLong Cheng

China Academy of Aerospace Standardization and Product Assurance, Beijing China, cheng.hailong@163.com

Wei Hou

China Academy of Aerospace Standardization and Product Assurance, Beijing China, 1009213017@qq.com

YaLong Wang

China Academy of Aerospace Standardization and Product Assurance, Beijing China, wangyl_708@163.com

With the continuous development of technology, traditional large-scale unmanned systems exhibit significant limitations when used for entertainment applications in urban airspace. These limitations include low visibility and insufficient visual impact. Moreover, individual products may face risks of being unavailable, unreliable, or even completely ineffective in environments with numerous electronic devices. Cluster unmanned systems based on backup complementary strategies can dynamically optimize their usage according to mission conditions. They can maintain better performance and cost-effectiveness in scenarios with functional variability and complex modes due to their strong resilience. Therefore, cluster unmanned systems have become a new application paradigm and have been widely used in corporate events and festivals, inevitably having a significant impact on future usage concepts. This paper reviews the progress of research on engineered resilient systems and cluster unmanned systems centered on drones. It deeply analyzes the connotations and interrelationships of resilience and security in cluster unmanned systems. Based on this, the paper uses the Markov model analysis method to verify the resilience of cluster unmanned systems and proposes corresponding safeguard strategies to provide theoretical support for the further development and application of related technologies.

Keywords: Cluster unmanned system, Resilience, Security, Backup complementary strategy.

1. Overview

Unmanned Aerial Vehicles (UAVs) offer flexibility, versatility, strong adaptability, and low cost, making them valuable in military and civilian applications. Cluster drones, which are groups of UAVs working together, enhance visual impact through coordinated efforts and collective intelligence, transforming traditional advertising methods. Their use in advertising has rapidly grown, significantly contributing to the low-altitude economy. For instance, in October 2024, a drone team from Shenzhen, China, deployed 6,000 drones to create a massive sky display in Saudi Arabia, showcasing cultural elements and evoking strong emotional responses from the audience. This innovative system is characterized by its low cost, anti-destruction capabilities, and intelligent features, paving the way for new low-

altitude economic opportunities. However, the rise of drone clusters also presents significant threats to key areas and events. With advancements in UAV intelligence and control technology, drone clusters are set to play a crucial role in the future of low-altitude economic development.

2. The Connotation of Resilience and Security of Cluster Unmanned Systems

2.1. *Resilience of Cluster Unmanned Systems*

2.1.1. *Connotation of Resilience*

The concept of resilience was first introduced by American ecologist Crawford S. Holling. Since then, various fields have researched resilience, defining it as the ability of a system to absorb and mitigate external shocks while maintaining its primary functions in hazardous conditions. Different disciplines emphasize various aspects of resilient systems. Some focus on the system's capacity to buffer against impacts, while others prioritize the system's ability to recover quickly after being affected.

In 2010, the U.S. Department of Defense proposed the concept of Engineered Resilient Systems (ERS). They defined a resilient system as one that is credible and effective, capable of being deployed immediately in diverse environments. Such a system can adapt to its external surroundings by reconfiguring its architecture or replacing components, with only minimal degradation in its detectable functions. Resilient systems are designed to maintain stable and efficient performance across a wide range of usage scenarios. When confronted with unknown risks from multiple sources, these systems can tolerate functional degradation within an acceptable range and can be integrated into other systems through reconfiguration or component replacement. Overall, resilient systems are easy to deploy and maintain, highly flexible in use, and provide good economic benefits.

2.1.2. *Connotation of Resilience*

In this concept, the essential elements of resilience in cluster unmanned systems include robustness, versatility, and restoration.

- **Robustness**: Under normal operating conditions, the cluster unmanned system can tolerate low-level disturbances while maintaining stable operations. This ensures minimal impact on its mission execution capabilities. For instance, if the system experiences minor electromagnetic interference or the loss of an individual unit within acceptable margins, it does not compromise communication and control among the cluster systems or hinder mission execution. Overall, such disturbances have no significant effect on the reliability of the system's tasks.
- **Versatility**: When faced with significant disturbances or environmental impacts, the cluster is capable of self-adjusting its system structure. It can dynamically assess the status of the cluster system and reconfigure its mission based on preset procedures and decision-making logic to optimize mission effectiveness. For instance, if strong electromagnetic interference or fire strikes cause certain systems within the cluster to lose their ability to execute missions, the remaining units can still carry out the planned mission. They achieve this by adjusting communication frequencies, reconfiguring mission execution units, and altering flight paths, thereby ensuring that the reliability of the cluster system's operations remains intact.
- **Restoration:** In the event of significant disturbances or fire strikes that result in multiple mission execution units losing their capabilities, the cluster system can swiftly identify the source of the failure. It can isolate severely impacted areas, assess the remaining capabilities, and leverage the cluster's redundant design and self-healing mechanisms to restore some of the lost functionalities through autonomous healing or dynamic reconfiguration. For example, if certain units within the cluster lose their mission execution capabilities, backup units can promptly fill those gaps. Additionally, the remaining systems can optimize and reconfigure themselves to quickly compensate for the lost capabilities, ensuring that the cluster system maintains its basic operational functionality.

In a cluster system with strong elastic capabilities, there is an inherent emergency response capacity. After unplanned disruptions, the system can recover through dynamic reconfiguration, as shown in Figure 1, which illustrates the relationship between its transformation process, robustness, versatility, and restoration.

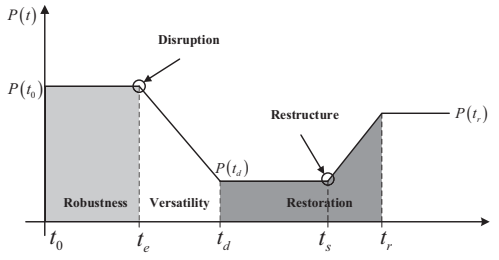


Fig. 1. This representation illustrates the resilience performance of a cluster system, highlighting its robustness, versatility, and restoration capabilities.

t_0 represents the system's overall performance, $P(t_0)$, under initial conditions. From t_0 to t_e, the cluster system remains stable or experiences minor disturbances while maintaining strong operational capabilities. At t_e, the system faces disruptions that lead to declining performance, but due to its resilience, it adapts and stabilizes by t_d, achieving performance $P(t_d)$. With redundancy and backups, the system implements recovery strategies between td and t_s, progressively restoring capabilities. By t_r, the system's capacity recovers to $P(t_r)$, which may match or be slightly lower than the initial performance $P(t_0)$.

2.2. *Security of Cluster Unmanned Systems*

2.2.1. *Connotation of Security*

The security of a product refers to its ability and features to protect people, equipment, and the environment from harm, damage, or negative effects caused by the product's own failures, malfunctions, misoperations, or other related factors. This consideration spans the entire product life cycle, including its design, manufacturing, use, and maintenance.

2.2.2. *Key elements of cluster unmanned system security*

Under this concept, the security of cluster unmanned systems refers to their ability to resist various intentional or unintentional security threats throughout their life cycle, ensuring that they are not illegally controlled, maliciously interfered with, or subject to data theft or tampering, and safeguarding the execution of missions without posing risks to the surrounding environment and personnel. The key elements mainly include information security, physical security, and mission security.

- **Information Security**: This text primarily addresses the security of communication and data transmission between the cluster and the ground control station, as well as among the individual units of the system. It includes key aspects such as data encryption, identity authentication, and access control. By implementing interference resistance, link encryption, and data encryption, the system prevents unauthorized devices from interfering with or accessing the cluster network. This ensures that the communication and control information of the unmanned system is protected from interception, tampering, or forgery by third parties.
- **Physical Security**: This safeguards the hardware components of the cluster of unmanned systems from physical attacks and electromagnetic damage. By utilizing strong casing designs, discreet deployment methods, and effective anti-attack measures, the system can endure various physical threats or reduce the extent of hardware damage.
- **Mission Security**: During mission execution, the system ensures that the actions of the cluster of unmanned systems align with the planned objectives. It also guarantees that basic or partial operational capabilities are maintained, preventing loss due to compromised information or physical security, which could otherwise impact the mission's success.

3.Relationship between resilience and security of cluster unmanned systems

3.1. *Mutual Promotion*

(i) Strong security is essential for a cluster of unmanned systems to achieve high resilience. Individual units must be equipped with effective measures to defend against both information and physical security threats. This is crucial for preventing interruptions caused by security vulnerabilities or susceptibility to destructive attacks. A well-secured system directly reflects its robustness, adaptability, and ability to recover from incidents.

(ii) A highly resilient cluster system can greatly improve its security. When an unmanned cluster system possesses strong capabilities to handle interference, adapt, and recover, it can quickly adjust its operations even if some units lose functionality. This is achieved through backup support or dynamic reconfiguration, which minimizes the impact of dangerous events and ensures mission security.

3.1. *Existence of conflicts*

(i) **Different focus areas**. Security design primarily emphasizes the defense and protection of products and missions. It prioritizes the closedness and controllability of individual units within the system. In contrast, resilience design focuses on the flexibility and adaptability of the entire cluster system. It does not concentrate on the performance of individual units; instead, it highlights the openness and dynamic reconfiguration capabilities of the whole cluster system.

(ii) **Resource competition**. In large-scale cluster drone display activities, significant resources are allocated to enhance system security through reliable communication, data encryption algorithms, and protection against electromagnetic interference. However, executing these tasks consumes computational resources, power, and communication bandwidth. This consumption can negatively impact the cluster system's ability to respond quickly to sudden environmental changes, leading to lower-than-expected resilience.

Therefore, when designing combat application scenarios for cluster unmanned systems, it is essential to strike a balance between flexibility and security. This balance ensures mission safety while allowing for effective responses to unexpected situations and accommodating the combat needs of various scenarios.

4. Resilience Verification Based on Markov Chains

There are usually two methods for evaluating the Resilience of general systems: experimental verification and theoretical analysis. This paper evaluates the resilience of cluster unmanned systems using a Markov model analysis due to the challenges posed by their large scale and complexity, which make experimentation difficult.

Cluster unmanned systems work in parallel small groups during task execution. Different tasks have varying resource and resilience requirements. This study measures resilience based solely on task success or failure. It assumes that each drone in the cluster operates in one of two states: task execution or failure, with failures occurring independently.

The high redundancy of functions among various systems within a cluster of unmanned systems is crucial for its resilience. When a specific task execution unit (or group) loses its ability to perform tasks, the system can reorganize the tactical structure of the remaining combat units to prevent task interruption caused by the loss of critical system performance.

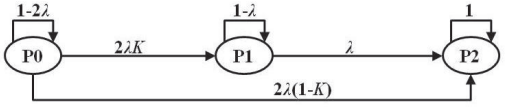
The number of drones required to complete the combat mission is i, the predetermined task execution unit (group) is G There are usually two methods for evaluating the Resilience of general systems: experimental verification and theoretical analysis. Due to the large scale and complex structure of cluster unmanned systems, and the difficulty of experimentation, this paper uses

Markov model analysis method to analyze and verify the resilience of cluster unmanned systems.

- P0: The scheduled task execution unit (group) is working normally;
- P1: If the scheduled task execution unit (group) fails, the task can continue to be executed with a lower success rate after system (task) reconstruction;
- P2: The scheduled task execution unit (group) has failed, and the redundant task execution unit (group) has also failed, but it can continue to execute the scheduled task after system (task) reconstruction
- P3: Both the scheduled task execution unit (group) and the redundant task execution unit (group) have failed, and the second-order redundant task execution unit (group) has malfunctioned, but the scheduled task can continue to be executed.
- P4: If the scheduled task execution unit (group) fails beyond repair, the redundant task execution unit (group) will continue to execute the scheduled task.
- P5: If both the scheduled task execution unit (group) and the redundant task execution unit (group) fail irreparable, the system will add another redundant task execution unit (group) to continue executing the scheduled task.
- P6: The scheduled task execution unit (group) and all redundant task execution units (groups) have experienced irreparable failures, resulting in task interruption.

4.1. *Single-Mode Redundant Elastic Model*

Assuming that each combat task unit within the system has only one redundancy, that is, the cluster unmanned system has only one redundant task execution unit (group), so there are only three states P0, P1, and P6, a single redundant task Markov Resilience model for the cluster unmanned system is established as follows.



Assuming that faults occur independently and follow an exponential distribution during task execution, the Markov Resilience model matrix is as follows:

$$\begin{bmatrix} M_0'(t) \\ M_1'(t) \\ M_2'(t) \end{bmatrix} = \begin{bmatrix} -2\lambda & 0 & 0 \\ 2\lambda K & -\lambda & 0 \\ 2\lambda(1-K) & \lambda & 0 \end{bmatrix} \cdot \begin{bmatrix} M_0(t) \\ M_1(t) \\ M_2(t) \end{bmatrix} \quad (1)$$

Among them, $\lambda$is the failure rate of task execution units;

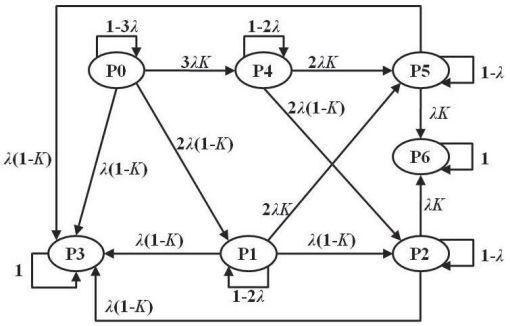
K is the coverage rate of system fault detection;

Assuming the initial state is P0, the initial condition in the equation is$M_0(0) = 1, M_1(0) = 0$， $M_2(0) = 0$, and the executable task rate of the dual redundant task structure Markov elastic model is

$$R_{SoS}(t) = M_0(t) + M_1(t) = (1-2K)\mathrm{e}^{-2\lambda t} + 2K\mathrm{e}^{-\lambda t}$$

4.2. *Dual-Mode Redundant Elastic Model*

If each combat task unit within the system has dual redundancy, meaning the cluster unmanned system contains two redundant task execution units (groups), establish a dual-mode redundant Markov Resilience model for combat tasks, as illustrated below.



The Markov Resilience model matrix is as follows:

$$\begin{bmatrix} M_0(t) \\ M_1(t) \\ M_2(t) \\ M_3(t) \\ M_4(t) \\ M_5(t) \\ M_6(t) \end{bmatrix} = \begin{bmatrix} -3\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 3\lambda K & -2\lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 2\lambda K & -\lambda & 0 & 2\lambda K & 0 & 0 \\ 0 & 0 & \lambda K & 0 & 0 & \lambda K & 0 \\ 2\lambda(1-K) & 0 & 0 & 0 & -2\lambda & 0 & 0 \\ 0 & 2\lambda(1-K) & 0 & 0 & \lambda(1-K) & -\lambda & 0 \\ \lambda(1-K) & 0 & \lambda(1-K) & 0 & \lambda(1-K) & \lambda(1-K) & 0 \end{bmatrix} \cdot \begin{bmatrix} M_0(t) \\ M_1(t) \\ M_2(t) \\ M_3(t) \\ M_4(t) \\ M_5(t) \\ M_6(t) \end{bmatrix} \quad (2)$$

Assuming the initial state is P0, the initial condition in the equation is$M_0(0) = 1, M_1(0) = 0$， $M_2(0) = 0, M_3(0) = 0, M_4(0) = 0, M_5(0) = 0, M_6(0) = 0$, and the executable task rate of the dual-mode redundant task structure Markov elastic model is

$$R_{SoS}(t) = M_0(t) + M_1(t) + M_2(t) + M_3(t) + M_4(t)$$

$$= (2K - K^2)\mathrm{e}^{-3\lambda t} + (2K^2 - 5K)\mathrm{e}^{-2\lambda t} + (1 + 3K - K^2)\mathrm{e}^{-\lambda t} \quad (3)$$

$\lambda = 2.8 \times 10^{-4}$/h .If the failure rate of the selected task execution unit is selected, the executable task rate of the dual redundant task structure Markov elastic model is shown in the following table.

Table 1. This table presents the executable task rates for both the Single-Mode Redundant Elastic Model and the Dual-Mode Redundant Elastic Model, evaluated under varying fault detection rates and total navigation durations.

Fault detection coverage rate K	Total flight time t/hour	Single-mode redundancy Ability	Dual-mode redundancy Ability
1	200	0.997	0.9998
	2000	0.8162	0.9212
0.9	200	0.9868	0.9946
	2000	0.7672	0.8956

The analysis reveals that there is a positive correlation between fault detection coverage and the redundancy level of task execution units with the task execution rate of the cluster unmanned system. Conversely, these factors are negatively correlated with the total flight hours. Longer task durations increase the risks associated with task completion, which also highlights the system's strong resilience. The system's ability to remain unaffected by interference leads to a higher success rate in achieving the established task goals.

5. Challenges faced by the resilience and security construction of cluster unmanned systems

Current research on cluster unmanned systems in the civilian market is still in the exploratory phase. In addition to providing highlights at large-scale events such as festivals and celebrations, these systems are integrating new technologies like augmented reality (AR) and virtual reality (VR) to enhance audience immersion. As a result, the collaborative design of resilience and safety in cluster unmanned systems faces significant challenges, including:

(i) Varied technical integration requirements and challenges in enhancing coordination efficiency within clusters.

As demand for diverse performance styles and imaging capabilities in cluster unmanned systems rises, the number of units in a cluster increases, complicating individual behavior control and coordinated flight. Ensuring resilience and safety in long-range operations requires high performance in flight range, speed, payload capacity, and sensor integration. It's vital to reduce reliance on less mature technologies while balancing individual safety and redundancy. The collaborative use of cluster drones involves decision-making theories from operations research, systems theory, computer science, intelligent algorithms, and communication principles. Autonomous decision-making in these systems is highly nonlinear and time-variable, creating strict resilience requirements. Current research needs further theoretical exploration and experimental validation for practical application. Thus, achieving real-time formation reorganization, trajectory planning, and optimal task allocation under high-altitude, high-speed, and variable conditions remains a significant challenge for building resilient systems that ensure mission safety and operational efficiency.

(ii) High Time-Variability of Topological Structures and the Urgent Need for Enhanced Top-Level Decision-Making

Most analyses on engineering resilience rely on reliability-oriented system safety, which has limitations in complex system design and verification. Traditional methods for identifying potential disturbances are influenced by human factors and perform well in static environments but struggle with sudden changes in dynamic operational settings. Cluster unmanned systems are designed with resilience, allowing them to maintain performance through task reconfiguration, even with some safety compromise. However, optimizing the information processing and decision-making system is essential. This system must real-time evaluate and allocate cluster capabilities and resources, balancing encryption, bandwidth, and decision-making. This dynamic optimization ensures smooth mission execution and maximizes resilience with limited resources, even during partial system failures.

(iii) Weak System Operational Resistance and the Need to Improve Communication Link Resilience

In complex urban environments, light pollution, electromagnetic radiation, and personal interference devices can disrupt communication between drones and ground stations, leading to data transmission failures. To address this, it is crucial to develop communication systems that use dynamic network adaptation technologies, ensuring efficient information transfer even amid interference and minimizing risks of property damage or personal injury. During long-range operations, widely distributed cluster unmanned systems face challenges due to limited signal transmission distance and data bandwidth, making it difficult to maintain effective point-to-point communication in large-scale, multi-task scenarios. Thus, building resilient communication links without compromising operational efficiency remains a significant challenge in this field.

5. Conclusion

The resilience and safety of cluster unmanned systems are essential for reliable operations and successful missions in complex environments. While research on their collaborative use is still developing, the intelligent use of these systems is becoming increasingly important.

By understanding the relationship between resilience and safety during the design phase and implementing targeted strategies, we can enhance operational performance and reduce mission costs. Future research must focus on strengthening resilience and improving safety mechanisms to address the evolving application requirements and security challenges. This will drive the transition of cluster unmanned systems from human-machine collaboration to dynamic perception and autonomous decision-making.

References

Kendoul, Farid (2012). Survey of Advances in Guidance, Navigation, and Control of Unmanned Rotorcraft Systems. *Journal of Field Robotics 29* (2): 315–378.

Al Arabiya News(2023). Saudi Arabia Deploys 6,000 Drones for Security and Surveillance. *Al Arabiya News*, October 15, 2023. https://www.alarabiya.net.

Sharma, Sumit, and Anil K. Singh (2020). Reliability and Safety Analysis of Swarm UAV Systems. *Journal of Aerospace Engineering 33* (4): 04020034.

Chen, Y., X. Wang, and L. Zhang(2019). Resilience and Fault Tolerance in Swarm UAV Networks. *IEEE Transactions on Vehicular Technology 68* (5): 4567–4578.

Khan, A., M. R. Khan, and S. A. Khan(2021). Enhancing the Security and Resilience of Drone Swarms: A Comprehensive Review. *Drones 5* (2): 35.

Holling, C. S.(1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics 4* (1): 1–23.

U.S. Department of Defense (2010). Emergency Response System (ERS): Policies and Procedures. Washington, DC: *U.S. Department of Defense*.

Zhang, X., Y. Li, and Z. Chen (2022). Resilient Control Strategies for UAV Swarms in Dynamic Environments. *Autonomous Robots 46* (3): 345–360.

Gupta, R., and S. Kumar(2019). Reliability and Safety in Multi-UAV Systems: A Probabilistic Approach. *International Journal of Robotics Research 38* (12-13): 1425–1440.

Kim, H., and J. Park (2020). Safety and Reliability Analysis of UAV Swarm Operations in Urban Environments. *Journal of Intelligent & Robotic Systems 100* (3-4): 987–1001.