방통융합정책연구 KMCC-2025-41

방송시설 보호를 위한 안티드론시스템 구축 방안 연구

(A Study on the Design Methodology of a C-UAS for the Protection of Broadcasting Facilities)

이승준/이영우/황철민

2025. 12

연구기관 : 주식회사 본레이크

방송미디어통신위원회
Korea Media and Communications Commission

이 보고서는 2025년도 방송미디어통신위원회 방송통신발전기금 방송통신 융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송미디어통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송미디어통신위원회 위원장 귀하

본 보고서를 **『방송시설 보호를 위한 안티드론시스템 구축 방안 연구』**의 연구결과보고서로 제출합니다.

2025년 12월

연구기관 : 주식회사 본레이크
총괄책임자 : 이승준
참여연구원 : 이영우, 황철민

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

방송시설 보호를 위한 안티드론시스템 구축방안 연구

2. 연구 목적 및 필요성

4차 산업의 드론 기술 발전으로 전시와 평시를 구분하지 않고 드론의 위협이 항상 상존한다. 특히 드론에 폭발물을 탑재하여 투하 및 자폭하는 공격은 적은 가격으로 기하급수적인 피해를 주는 유형으로, 이에 대한 사전 대처로 방송시설의 안티드론 시스템 구축이 반드시 논의되어야 한다.

하지만 방송시설에 안티드론 시스템을 구축하기 위해서는 해결해야 할 요소가 다수 존재하며, 이는 다음과 같다.

○ 방송시설 안티드론 시스템의 부작용(전파 방사, 요격으로 인한 2차 피해)

○ 안티드론 시스템 운용 주체의 모호함(방송시설, 군, 경, 대테러센터 등)

○ 무력화를 사용 권한에 대한 법제의 부재

○ 무력화를 사용한 이후 2차 피해에 대한 책임·면책에 대한 법제의 부재

외부 노출도가 높고 전파 환경에 민감한 방송시설의 특성은 안티드론 시스템 구축과 법제 도입에 큰 제약을 주고 있으며, 이를 완화하기 위한 연구가 필요하다.

3. 연구의 구성 및 범위

본 연구는 위험 분석(Risk Analysis) 기법을 이용하여 방송시설의 적합한 안티드론 시스템을 도출하고 이를 운용, 정책, 제도적으로 활용할 수 있는 방안을 제시한다.

위험 분석의 과정과 도출되는 결과는 다음과 같다.

① 방송시설 상황 설정 단계 → 방송시설의 현재 상황

② 방송시설 위험 식별 단계 → 방송시설 위협 시나리오

③ 방송시설 위험 분석 단계 → 위험 수준 산정표

④ 방송시설 위험 평가 단계 → 위험 허용 기준에 따른 방송시설의 위험 수준

⑤ 방송시설 위험 대응 단계 → 안티드론 시스템 도입에 따른 위험 수준의 변화

이를 통해 안티드론 시스템의 도입에 따라서 방송시설의 위험 수준이 어떻게 변화하는지 알 수 있으며, 도입해야 할 최소·최적·최대의 안티드론 시스템을 판단하는 기준을 제공한다. 이후 다음과 같은 안티드론 구축 방안의 세 가지 핵심 요소를 제시한다.

① 방송시설 안티드론 시스템 선정 방안

② 방송시설 안티드론 시스템 배치 방안

③ 방송시설 안티드론 시스템 운용 방안

이를 통해 안티드론 시스템 구축을 위한 인증·운용·정책·법제 전반의 방향 설정에 참고 자료로 활용될 수 있다.

4. 연구 내용 및 결과

가. 연구 배경

안티드론 시스템은 탐지→식별→무력화의 과정으로 드론을 방어한다. 하지만 전파환경에 민감하고 안테나가 외부에 노출된 방송시설의 취약성으로 인해 드론의 위협뿐만 아니라 안티드론 시스템 그 자체로도 위협이 될 수 있으며, 이는 다음과 같다.

○ 탐지 시스템의 방송시설 위협

탐지 유형	방송시설 위협 여부	비고
RF 탐지	매우 낮음	수동 수신 방식, 전파 방사 없음
EO/IR 탐지	매우 낮음	전파 영향 없음
음향 탐지	제외	실질적 운용 한계
레이다 탐지	높음	고출력 전파 방사, 혼신 가능성

○ 무력화 시스템의 방송시설 위협

유형	종류		설명	위협 여부
하드킬	레이저		고출력 레이저로 파괴	높음
	HPM		고출력 마이크로파로 파괴	높음
	그물		발사형 그물로 비행 불능	높음
	요격드론		직접 접근하여 충돌 파괴	높음
소프트킬	단순	전방위 재밍	광역 전파 방해	높음
		지향성 재밍	특정 방향 전파 방해	높음
		GPS 스푸핑	위성항법(GNSS) 신호를 기만	높음
	정밀	스마트 재밍	선택적 주파수/시간 방해	매우 낮음
		정밀통제형	드론의 제어권을 탈취하여 통제	매우 낮음

종합하면 탐지에서는 ‘레이다’, 무력화에서는 드론의 진입을 막는 ‘단순 소프트킬’과 드론을 물리적으로 파괴하는 ‘하드킬’ 방식의 사용은 방송시설에서 부작용을 항시 동반한다.

나. 위험 분석의 내용 및 결과

본 연구는 방송시설의 자산을 물리적 피해를 입을 수 있는 ‘유형 자산(6)’과 전파로 인한 피해를 받을 수 있는 ‘무형 자산(10)’으로 구별하여 총 16개의 자산을 도출하였다.

이후 방송시설을 위협할 수 있는 유형을 ‘적대적 공격(5)’, ‘우발적 사고(2)’, ‘부수적 피해(4)’로 구별하여 총 11개의 위협 리스트를 도출하였다.

각 자산과 위협의 조건을 통해 총 60개의 ‘위협 시나리오’를 도출하였고, 각 시나리오에 대한 ‘영향도’와 ‘발생 가능성’을 도출하여, 각 위협 시나리오에 대한 ‘위험 수준’을 도출하였다.

위험 수준을 ‘위험 허용 기준’과 방송시설에 설치될 확률이 높다고 판단되는 ‘방어 체계’에 대입하여 위험 평가를 실시한 결과의 요약은 다음과 같다.

○ 위험 평가 결과 요약

방송시설은 현재 즉각적으로 도입할 수 있는 수동형 탐지 시스템의 구축이 우선적으로 요구된다. 이를 통해 군·경 등의 유관 기관 연계를 통해 드론에 대한 대응 수단을 확보할 수 있다. 또한 전파 환경에 민감한 방송시설에서는 단순 소프트킬보다 정밀 소프트킬이

방송서비스 측면에서 위험 저감 효과가 크다. 하드킬 체계에서는 수동형 탐지보다 레이다와 같은 능동형 탐지 장비가 요격 통제 및 즉각 대응 단계에서 위험 저감 효과가 크다. 하지만 레이다는 전파 방사의 부작용이 동시에 존재한다.

다. 안티드론 시스템 구축 방안의 내용 및 결과

위험 분석 결과를 바탕으로 단계적으로 방송시설에 도입할 수 있는 안티드론 시스템 3종을 기준 모델로 선정하였다. 시스템 선정에는 법적 허용 범위, 요구 방어 범위·대응 수준, 운용 부작용 및 주변 영향, 방송 장비와의 상호운영성, 전자기·전파 환경 호환성을 종합 고려하였다. 특히 고출력 송신 설비와 다종 무선 시스템이 밀집된 방송시설 특성을 반영하여, 방송 주파수 간섭 및 송출 장애를 유발하지 않는 것을 핵심 전제로 설정하였다.

○ RF 스캐너, 카메라 센서(EO/IR) 기반의 수동형 탐지 체계

- 선정 이유: 전파 차단 등 능동 대응이 없어 현행 제도 하 적용 용이, 조기 탐지·상황 인지에 적합, 대응은 군·경 연계 중심

○ RF 스캐너, 카메라 센서(EO/IR) 기반의 정밀 소프트킬 체계

- 선정 이유: 정밀 운용을 전제로 대응 수단 확보, 운용 시간·주파수 정합 제어로 방송 간섭 최소화 가능, 다만 혼신 등 부작용 가능성을 고려한 인증·제도 필요

○ 레이다, 카메라 센서(EO/IR) 기반의 하드킬 체계

- 선정 이유: 드론 항법 방식 의존성이 낮아 즉각 대응 가능, 다만 물리적 요격에 따른 법적 책임·사회적 수용성 및 2차 피해 위험을 고려해 제한적 적용이 적합

배치 측면에서는 방송시설의 전파 환경과 안전성을 고려할 때, 안티드론 시스템은 장비 성능 중심의 설치가 아니라 전파 간섭 회피와 음영 구역 최소화를 전제로 한 기능 중심 배치가 필요하다는 결과가 도출되었다. 이에 따라 탐지 장비는 시설 접근 방향과 지형 특성을 반영하여 단일 또는 다중 세트로 구성하고, 무력화 장비는 방송송출 설비와 이격된 위치에서 대응 방향과 범위를 명확히 제한하는 방식이 적합한 것으로 평가되었다. 특히 물리적 요격을 수반하는 체계는 광범위한 배치보다 운용 범위를 한정한 단일 세트 배치가 현실적인 것으로 나타났다.

운용 측면에서는 제도적 문제로 방송시설 단독 대응에는 한계가 존재하므로, 외부 협력기관과의 연동을 전제로 한 역할 분담형 운용 구조가 필수적인 결과로 도출되었다. 방송시설은 탐지·상황 인지·정보 제공을 중심으로 운용하고, 공권력적 조치는 군·경 등 외부 기관이 주도하는 방식이 법적·제도적 부담을 최소화하는 것으로 평가되었다. 또한 방

송시설 간에는 제조사나 장비 종류에 종속되지 않는 통합 관제 기반의 공동 운용 체계가 필요하며, 이를 통해 위협 상황을 일관된 기준으로 관리할 수 있는 것으로 분석되었다.

5. 정책적 활용 내용

○ 방송시설 안티드론 정책 검토 자료로 활용

- 방송시설은 방호 의무에 비해 실질적 드론 대응 권한이 제한되어 있어, 안티드론 관련 법·제도 보완의 필요성을 검토하는 정책 기초 자료로 활용 가능
- 방송송출 안정성과 드론 대응 간의 구조적 충돌 관계를 정리하여, 향후 제도 개선 논의의 근거자료로 활용 가능

○ 단계적 제도 도입 및 운용 모델 설계에 활용

- 탐지 자산 우선 구축과 외부 기관 연계 대응 등 현행 제도 내에서 적용 가능한 단계적 도입 전략 수립에 활용 가능
- 기술적 안전성 검증을 전제로 한 인증·운용 기준 마련과 민·관·경 협력 모델 설계 시 참고 자료로 활용 가능

6. 기대효과

○ 방송시설 보호체계 고도화

- 방송시설의 전파 환경과 운용 특성을 반영한 위험 분석과 단계적 안티드론 대응 모델을 제시함으로써, 방송송출 안정성을 저해하지 않으면서도 실질적인 드론 위협 대응이 가능한 보호체계 구축 기반 마련

○ 정책·제도 정비의 기준 제시

- 방송시설 안티드론 운용 과정에서 발생하는 법·제도적 공백을 구조적으로 정리하고, 기술적 안전성 입증을 전제로 한 단계적 제도 도입 방향을 제시함으로써 향후 관련 정책·제도 개선을 위한 참고 자료로 활용

○ 후속 실증 및 연구 연계 기반 마련

- 방송시설 대상 한 위험 요소를 체계적으로 분석·정리함으로써, 향후 정량적 위험 평가, 데이터 기반 확률 모델, 실증 연구 등 고도화하기 위한 기초 자료로 활용

SUMMARY

1. Title

A Study on the Design Methodology of a C-UAS for the Protection of Broadcasting Facilities

2. Objective and Importance of Research

Recently, With the advancement of drone technologies, drone-related threats have become persistent risks in both peacetime and wartime environments. In particular, attacks involving explosive-laden drones, including payload drops and suicide missions, represent low-cost but high-impact threats capable of causing disproportionate damage. As a preventive measure, the establishment of C-UAS systems for broadcasting facilities must be seriously considered.

However, broadcasting facilities face unique challenges in adopting C-UAS systems. These include potential electromagnetic interference and secondary damage caused by interception, ambiguity regarding operational authority among broadcasting operators and public security agencies, the absence of a legal framework governing the use of neutralization measures, and the lack of legal provisions addressing liability for secondary damage. Broadcasting facilities are physically exposed and highly sensitive to radio and electromagnetic interference. As a result, they face substantial technical and institutional constraints that significantly limit the deployment and operation of C-UAS.

3. Contents and Scope of the Research

This study applies a risk analysis methodology to identify C-UAS systems suitable for broadcasting facilities and to propose operational, policy, and institutional utilization strategies. The risk analysis process consists of defining facility contexts, identifying threat scenarios, analyzing and evaluating risk levels, and assessing changes in risk resulting from the introduction of C-UAS systems.

Through this process, the study provides criteria for determining the minimum, optimal, and maximum levels of C-UAS system deployment. Based on the analysis results, three key elements are presented:

(1) Selection criteria for C-UAS systems,

(2) Broadcasting facility specific deployment strategies

(3) Risk aware operational strategies

This study aims to support informed decision-making in the operational deployment, policy development, and legal and institutional aspects of C-UAS systems in broadcasting.

4. Research Results

A. Risk Characteristics of Broadcasting Facilities

Broadcasting facilities are inherently vulnerable due to external antenna exposure and sensitivity to electromagnetic interference. While passive detection technologies such as RF-based and EO/IR-based detection pose minimal risk, radar-based detection systems involve high-power emissions and present significant interference risks.

Similarly, hard-kill neutralization methods and simple soft-kill techniques involving wide-area radio frequency disruption pose substantial risks to broadcasting services. In contrast, precision soft-kill approaches, when properly controlled, were assessed as having relatively low impact on broadcasting operations.

Overall, radar-based detection, simple soft-kill methods, and hard-kill approaches were

identified as being accompanied by unavoidable operational side effects in broadcasting environments.

B. Risk Analysis Results

The study classified broadcasting facility assets into six tangible assets and ten intangible assets, and identified eleven threat categories encompassing hostile attacks, accidental incidents, and collateral damage. Based on these factors, sixty threat scenarios were derived and evaluated in terms of impact and likelihood.

The results indicate that broadcasting facilities can secure initial response capabilities through the deployment of passive detection systems in coordination with external authorities under the current legal framework. In electromagnetic-sensitive environments, precision soft-kill systems were found to be more effective in reducing service-related risks than simple soft-kill methods. Although radar-based detection enhances response effectiveness for hard-kill systems, the associated electromagnetic risks remain a significant concern.

C. Deployment and Operational Implications

The study identified three C-UAS system types with high applicability to broadcasting facilities, selected based on legal permissibility, operational impact, interoperability, and electromagnetic compatibility. Avoiding broadcast frequency interference was established as a core prerequisite.

Deployment strategies should prioritize function-oriented placement, emphasizing interference avoidance and blind-spot minimization rather than equipment performance alone. Detection systems may be deployed in single or multiple sets depending on site characteristics, while neutralization systems should be installed at locations sufficiently separated from broadcasting transmission facilities. For physically interceptive systems, limited-range, single-set deployment was found to be the most realistic approach.

Operationally, broadcasting facilities face limitations in conducting standalone responses. Accordingly, a role-sharing operational structure coordinated with external agencies is essential. Broadcasting facilities should focus on detection and situational awareness, while coercive measures should be executed by authorized public institutions. In addition, a manufacturer-independent integrated monitoring framework is required to ensure consistent threat management across facilities.

5. Policy Suggestions for Practical Use

This study can be utilized as a reference for reviewing and improving C-UAS policies for broadcasting facilities, particularly in addressing the gap between protection obligations and response authority. By clarifying structural conflicts between broadcasting stability and drone countermeasures, it supports future institutional reform discussions.

Furthermore, the study provides a basis for designing phased adoption strategies within the current legal framework, prioritizing detection assets and coordinated responses, as well as for developing certification standards and cooperative governance models involving public and private stakeholders.

6. Expectations

The study contributes to the advancement of broadcasting facility protection systems by presenting risk-based, phased C-UAS response models that preserve transmission stability. It also offers a benchmark for policy and institutional improvement by systematically identifying legal and regulatory gaps and proposing safety-verified implementation pathways. Finally, the structured analysis of risk factors provides foundational data for future quantitative risk assessments, empirical validation, and follow-up research.

CONTENTS

제1장 서 론

제1절 연구 배경 및 목적

1. 연구 배경

가. 드론 기술 발전의 양면성

〔그림 1-1〕 2025년 누구나 드론을 쉽게 접근할 수 있는 시대

4차 산업혁명의 가속화로 다양한 기술이 일상생활에 깊숙이 자리 잡고 있으며, 그중 드론 기술은 상용화와 생산 비용 감소를 통해 빠르게 대중화되고 있다. 드론은 항공 촬영, 물류 배송, 시설 점검, 재난 대응 등 여러 산업 분야에서 활용되며 국민 생활의 편의성과 산업적 효율성을 높이는 핵심 기술로 자리매김하고 있다. 나아가 공공 분야와 안전 관리 영역에서도 감시·정찰, 출입 통제, 침입 방지와 같은 임무에 적용되며 활용 가치가 확대되고 있다. 이러한 변화와 함께 드론은 더 이상 특정 목적을 위한 전문 장비가 아니라 사회 전반에서 폭넓게 사용되는 일상적 기술로 자리 잡고 있다.

그러나 이러한 긍정적 발전과 병행하여 드론의 악용 가능성 또한 빠르게 증가하고 있다.

소형·저소음·저가화된 상업용 드론은 누구나 손쉽게 접근할 수 있으며, 은밀하게 이동하거나 다양한 방식으로 활용될 수 있어 악의적 목적에 이용되기 쉽다. 그 결과 단순한 사생활 침해 수준의 불법 촬영을 넘어 공공시설 침투, 정보 수집, 폭발물 투하 등 국가안보를 위협하는 심각한 공격 행위로 발전하고 있다. 이러한 변화는 드론이 산업 분야에서만 활용되는 장비가 아니라, 공격 목적으로 악용될 수 있음을 보여준다. 이에 따라 드론 기반 테러에 대비하기 위한 체계적 대응 기술과 방호체계의 필요성이 점차 커지고 있다.

나. 드론을 이용한 비대칭 위협 급부상

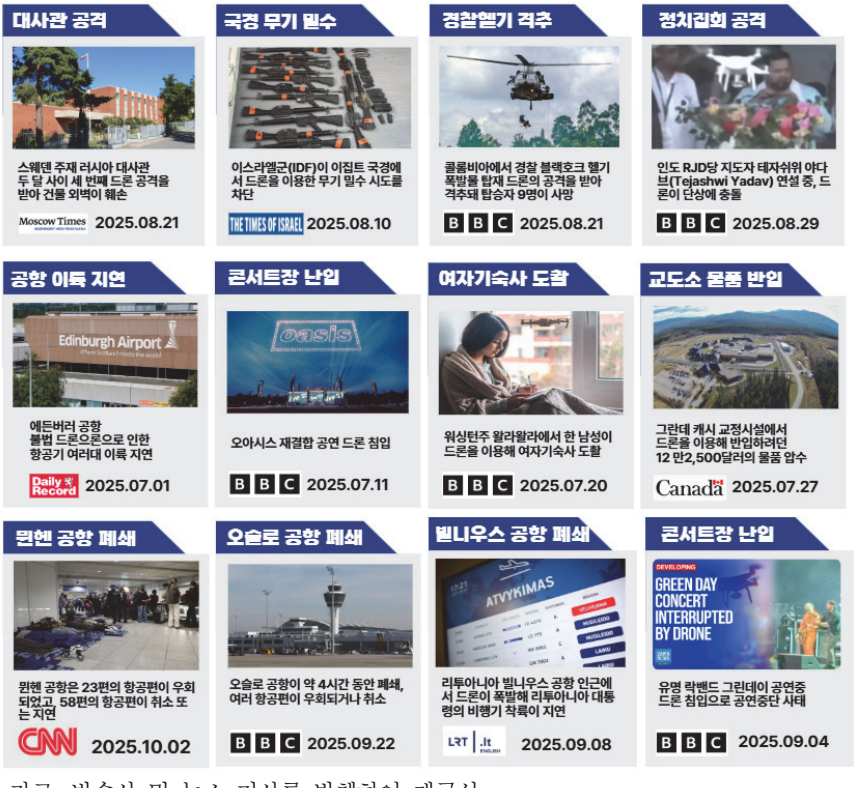
〔그림 1-2〕 새로운 안보 위협으로 급부상 중인 드론

드론을 활용한 위협은 전 세계적으로 꾸준히 발생하며 그 심각성이 점차 분명해지고 있다. 2014년 프랑스 원전 주변에서 정체불명의 드론이 여러 차례 출몰한 사건과 2015년 미국 백악관 상공에서 드론이 추락한 사고는 해외 주요 국가기관이 드론 침투 위험에 직면해 있음을 보여준다. 2018년 영국 개트윅 공항 활주로 부근에서는 드론 출몰로 모든 항공기의 이착륙이 중단되는 사건이 발생하였으며, 이는 드론 한 대만으로도 대규모 공항 운영이 마비될 수 있음을 확인시킨 대표적인 사례이다. 최근에는 2025년 스웨덴 고텐버그 공항에서 드론이 활주로 인근에서 포착되며 공항 운영이 일시 중단되는 사건이 발생하였다. 이는 드론의 출몰만으로도 국제공항의 항공안전과 운영 연속성이 즉각 위협받을 수 있음을 보여주는 사례이다. 이러한 해외 사례들은 드론이 국가 주요시설과 사회기반시설

의 운영에 중대한 영향을 미칠 수 있음을 보여주며 이러한 위험은 국내에서도 동일하게 발생하고 있다.

2024년 대통령실 주변에서 불법 드론이 발견된 사례가 있었으며, 국가정보원 청사를 촬영하던 외국인이 체포되는 사건도 보고되는 등 주요 국가기관과 중요시설을 대상으로 한 침입 시도가 이어지고 있다. 이 같은 사례들은 드론 위협이 단순한 사생활 침해 수준을 넘어 국가안보와 사회기반시설의 안정성에 실질적인 위험을 초래할 수 있음을 보여준다. 이러한 상황에서 드론 위협에 취약한 대상은 군사 시설에만 국한되지 않으며, 국가기반시설 전반이 잠재적 공격 표적이 되고 있다. 특히 방송시설은 국가재난·비상상황에서 국민에게 정보를 전달하는 핵심 기반시설임에도 불구하고 드론 위협에 대한 대응 기준과 체계는 여전히 부족하다.

〔그림 1-3〕 2025년 하반기 드론 위협



자료: 방송사 및 뉴스 기사를 발췌하여 재구성

다. 현대 하이브리드 위협에서의 방송시설보호 중요성 증대

과거 역사적 흐름을 살펴보면, 항상 전쟁에서의 전통적 무기의 발전에 있어 새로운 기술적 변화가 등장하였다. 그러나 이 새로운 무기의 발전은 20세기에 들어 군사적 수단보다 비군사적 방법의 영향력이 더욱 커지기 시작하였다. 실제로 히틀러의 측근이었던 알베르트 슈페어는 뉘른베르크 재판 과정에서, 라디오와 확성기와 같은 대중 매체가 독일 사회 전반의 사고와 판단을 약화시키는 데 핵심적 역할을 했음을 인정하였다[23].

이처럼 제2차 세계대전 이후에는 정보전과 심리전을 포함하는 차세대 전쟁 양식, 즉 하이브리드 전쟁에 대한 연구가 지속적으로 이루어져 왔다[24]. 하이브리드 전쟁은 군사·비군사 수단을 복합적으로 활용함으로써, 그 위협성과 파급 효과 면에서 가장 높은 위험성을 지닌 전쟁 형태로 평가된다[1].

현대 하이브리드 전쟁의 양상 속에서 방송시설은 단순한 언론 매체를 넘어, 전쟁의 승패를 가르는 전략적 중심(Center of Gravity)으로 급부상하였다.[1] 현대전의 목표가 적의 영토 점령에서 '적의 의지 마비'와 '사회적 혼란 유도'로 이동함에 따라, 대중에게 정보를 전달하는 유일한 통로인 방송망은 공격자에게 가장 매력적인 표적이 되었기 때문이다. 방송시설이 무력화될 경우, 정부는 국민에게 정확한 재난 정보를 전달할 수 없게 되며, 그 공백을 틈타 가짜 뉴스를 유포하여 내부 분열을 획책할 수 있다.

특히 최근 드론과 같은 무인 무기체계의 등장은 하이브리드 전술을 완성하는 기폭제가 되었다. 드론은 저비용으로 고가치 자산을 정밀 타격할 수 있는 효율적 '비대칭 전력'이자, 공격 주체를 은폐하며 적의 후방 깊숙한 곳에 위치한 핵심 인프라를 타격할 수 있는 최적 수단으로 자리 잡았다. 이로 인해 방송시설은 기존 방어체계만으로는 대응하기 어려운 입체적인 위협에 직면하였으며, 이는 전장 환경의 구조적 변화를 가속화시키고 있다.

1) 현대전에서의 방송시설 타격 사례

2022년 3월 1일, 러시아군은 우크라이나 침공 직후 수도 키이우의 TV 타워를 가장 먼저 타격하였다.[2] 당시 러시아 국방부는 이를 '정보공격'을 위한 작전이라고 공식 발표

1) Hybrid Threat Center of Gravity Analysis: Taking a Fresh Look at ISIL, Joint Force Quarterly, No. 84, National Defense University Press, 2017.01.26.

〔그림 1-4〕 러시아 군의 우크라이나 TV 방송 타워 공격

자료: MoneyS

하며 방송시설을 핵심 군사 목표물로 간주하였다. 이 공격으로 인해 우크라이나의 국영 방송송출이 일시 중단되었으며, 이는 현대전에서 적국이 국민의 눈과 귀를 가리기 위해 방송인프라를 최우선 타격 순위로 설정하고 있음을 시사한다.

2021년 5월 이스라엘-팔레스타인 분쟁 당시 AP통신과 알자지라 방송국이 입주한 알 자라(Al-Jalaa) 타워를 드론과 미사일로 파괴했던 전례가 있으며,[3] 이후 현대전은 방송시설을 적의 정보 거점으로 간주하여 선제적으로 무력화시키는 전략의 변화가 시작되었다.

2023년 10월 이스라엘-하마스 전쟁 발발 직후에는 가자지구 내 주요 미디어 매체와 송출 장비가 집적된 가자지구 언론사 건물들의 방송 및 통신 인프라를 무력화하였다. 특히 '팔레스타인 타워' 는 다수의 현지 언론사, 방송 제작사, 라디오 방송국, 인터넷 서비스

2) 우크라 TV타워 파괴, 국영방송 마비...러시아 고정밀 타격, NOWnews, 2022.03.02.

3) 가자지구 외신 입주 건물 폭격한 이스라엘… 알자지라 '살상 은폐하려, 한국일보, 2021.05.16.

제공 업체들이 입주해 있어 사실상 가자지구의 미디어 센터 역할을 하고 있었다. 하지만 이스라엘군은 이 건물이 겉으로는 언론사이지만, 실제로는 하마스의 군사 정보 부서와 통신 네트워크를 위한 핵심 인프라로 사용되고 있다고 주장하였으며, 특히 이 건물에 하마스의 정보 부대가 입주해 있으며, 특히 'GPS 교란 장비'를 운영하여 이스라엘군의 정밀 유도 무기를 방해하고 있다고 주장했다.[4)]

〔그림 1-5〕 2023년 가자지구의 미디어 타워 및 송신탑 붕괴

자료: Associated Press

2) 소형 자폭 드론을 이용한 방송시설 타격 사례

2024년 7월, 러시아 서부 쿠르스크주 수자(Sudzha) 지역의 방송송출탑이 우크라이나군의 두 대의 드론 공격을 받아 화재가 발생하였다. 이로 인해 해당 지역의 디지털 방송송출이 중단되었다.[5)]

2025년 11월, 우크라이나 공영방송인 수스필네 드니프로(Suspilne Dnipro)와 우크라이나 라디오 드니프로가 입주한 편집국 건물이 심각한 피해를 입었다. 저가 자폭 드론을 동

4) Electronic warfare: Israel ramps up GPS jamming to counter Hamas drone attacks, FRANCE 24, 2023.10.17.

5) Russian Kursk Oblast authorities report UAV attack on TV tower and gas station, Ukrainska Pravda, 2024.07.14.

시·연속적으로 투입하는 전형적인 드론 기반 공격 형태로 언론·방송 시설이 핵심이 되었다.[6] 메인 스튜디오는 전소되었으며, 텔레비전 송신탑 등이 파괴되었다. 이처럼 최근에는 드론을 이용하여 방송시설을 타격하여, 저비용으로 심리적 압박을 가할 수 있다는 점에서 자폭 드론은 현대 전장에서 심리전과 결합된 새로운 형태의 위협이 급부상하고 있다.

〔그림 1-6〕 15개의 자폭 드론으로 전소된 우크라이나 공영방송국 스튜디오

자료: Lenta.RU(2024.07.), DW Akademie(2025.11.) 뉴스 기사 발췌

6) "Everything burned down" : Dnipro media facilities destroyed as 15 drones strike city, two injured, Euromaidan Press, 2025.11.18.

라. 방송시설의 법적 지위와 방어의 중요성

이와 같은 국제적 안보 환경 변화 속에서 대한민국 방송시설의 방어는 단순한 시설 보호를 넘어 국가 안보와 직결된 핵심 과제이다. 방송시설은 「방송통신발전 기본법」 제40조에 의거하여 평시 각종 재난 상황 발생 시 국민의 생명과 안전을 보호하기 위해 관련 정보를 '정확하고 신속하게' 전달해야 할 법적 의무가 부여된 국가 핵심 인프라이다.[7] 특히 전시 또는 국가 비상사태 시에도 민방위 경보와 지휘·통제 정보를 전파하는 전략적 정보 전달 수단으로 기능하기 때문에, 방송 기능의 중단은 곧 대국민 안전 저해와 국가 안보상의 치명적인 정보 공백은 안보의 공백으로 직결된다. 이러한 중요성을 반영하여 정부는 방송시설을 「국가중요시설 지정 및 방호 훈령」에 따라 대통령 집무실, 국회의사당 등과 함께 국가중요시설로 지정·관리하고 있다. 이는 방송시설이 현대 안보 환경에서 단순한 공공 인프라가 아니라, 하이브리드 전쟁에 대응하기 위한 핵심 방어 대상임을 제도적으로 인식한것이라 할 수 있다.

마. 방송 송신 시설의 구조적 전파환경 특수성

일반적으로 안티드론과 같은 보안 시스템 구축 시 시설만이 가지는 특수한 환경 및 운영 조건을 전제로, 위협의 기준과 적용의 제약, 그리고 실질적인 방호 절차 및 구축방법론이 요구된다. 특히 방송시설은 국가 중요시설 중에서도 구조적 특성과 전파환경의 특성이 아주 민감한 특수한 환경이다. 따라서 일반적인 국가 중요시설 방호 대책을 일률적으로 적용할 수 없으며, 드론 공격과 부작용을 모두 고려한 방송시설 특화된 '이중 리스크 관리 모델'이 요구된다.

1) 방송시설의 구조적 특성과 드론 공격

특히 방송 송신 시설은 전파 효율성을 위해 산 정상이나 도심의 개방된 건물 위 고지대에 위치하며, 안테나, 급전선, 철탑 구조물 등 핵심 자산이 물리적 방어 없이 공중에 완전히 노출되어 있다는 구조적 취약성을 가진다. 이는 적대적 드론의 접근 경로상 시야(LOS)

7) 방송통신발전 기본법 제40조(재난방송 등)

가 확보되기 쉽고, 복잡한 침투 과정 없이 소형 자폭 드론의 물리적 타격에 무방비로 노출될 수 있음을 의미한다.

2) 방송시설의 전파 환경 특성과 대응

방송 송신 시설 환경에서 무분별한 안티드론 대응 역시 심각한 2차 피해를 초래할 수 있다. 안티드론 재머 가동 시 방송 장비 시스템의 신뢰성이 저하, 재밍 기반 대응은 GPS 시각 동기화 붕괴, 송신 품질 저하, 광역 방송 중단 등 자기 파괴적 결과를 유발할 가능성이 높다. 이는 적 드론의 공격이 발생하지 않더라도, 대응 과정 자체가 방송서비스의 연속성과 공공 안전을 훼손하는 역설적 상황을 초래할 수 있음을 의미한다.

2. 연구 동향

1) 구축방안 연구

곽해용(2021)은 국가중요시설의 안티드론 시스템 구축 시 우선 고려해야 할 영향 요인을 AHP(계층화 분석법)를 통해 실증적으로 분석하고, 시설 등급별 최적화된 대응 방안을 제시하였다. 분석 결과, 전문가들은 '다수 표적(군집 드론)에 대한 동시 탐지 및 차단'을 가장 시급한 핵심 성능으로 꼽았으며, 시설 관계자들은 2차 피해를 최소화하는 소프트킬(Soft-kill) 능력을 선호하는 것으로 나타났다. 이를 바탕으로 연구는 국가중요시설의 중요도에 따라 차등화된 시스템 구성을 제안하였다.[2]

송채근・김형석(2025)은 국내 상용 드론 35종의 탑재 중량과 비행속도를 변수로 한 정량적 위험성 평가를 통해 드론 위협을 4등급(최고・고・중・저)으로 분류하고, 이를 바탕으로 국가중요시설 방호를 위한 3지대 기반으로 전략을 제시하였다. 본 연구는 폭발물 파편 안전거리와 최소 대응 시간을 통합 고려하여 1차(15km)・2차(5km)・3차(2.5km)로 방호지대를 설정하였으며, 위험군별 특성에 최적화된 차별적 방호전략을 제안하였다.[3]

김태영(2020)은 위험평가 이론을 개념적 틀로 적용하여 국내 방호체계의 구조적 한계를 분석하고 정책적 개선방안을 제시한 연구이다. 저자들은 드론 테러 사례와 제도 현황을 바탕으로 국가중요시설 방호가 기관별로 분절되고, 드론을 고려한 설계기준위협(DBT), 통합 물리 방호체계, 탐지・대응 수단, 공역통제, 법・제도적 근거가 미흡하다고 지적하며,

이에 대한 개선책으로 DBT 기반 통합 방호체계 구축, 안티드론 시스템 확대와 대응 매뉴얼 정립, 중요도 기반 공역통제 및 드론 비행관리체계 개선, 전파차단·격추 등 대응을 뒷받침하는 법령 개정을 제안한다. 이 연구는 실제 자산식별이나 위협·취약성 평가를 수행한 것이 아니라, 위험평가모형을 정책 분석과 제도 개선을 위한 도구로 활용의 필요성을 제안하였다.[4]

황순필·김두환(2020)은 국가중요시설 방호를 위한 기존 안티드론 논의가 원론적인 수준에 머물러 있음을 지적하며, 문헌 연구와 전문가 심층 인터뷰를 통해 실무에 적용 가능한 중첩·복합적 대응체계 구축 방안을 제시하였다. 연구 결과, 단일 센서의 한계를 극복하기 위해 다각적 센서를 중첩·혼합 운용하여 탐지율을 극대화하고, 무력화 단계에서는 소프트킬과 하드킬 수단을 다중 배치하여 작전 환경에 따른 유연한 대응체계를 갖출 것을 제안하였다.[5]

이유빈·류세환·윤진섭(2023)은 국가중요시설인 다목적댐 및 부속 시설을 대상으로 불법 드론의 위협에 선제적으로 대응하기 위한 안티드론 시스템 구축 방안을 제시하였다. 본 연구는 댐 시설이 접경지역이나 산악지형에 위치하고, 민간인 출입이 잦은 개방형 구조라는 점에 주목하여 현장 여건을 고려한 기술 도입 방안을 검토하였다. 연구 결과, 자율비행과 원격조종 드론을 모두 탐지하기 위해 레이다와 EO/IR을 연동한 복합탐지 체계를 구축할 것을 제안하였으며, 탐지부터 무력화까지 통합 제어할 수 있는 모니터링 시스템 개발과 기관 간 협력·공유체계 구축을 제안하였다.[6]

이동준·정길현·권형안·양상운(2021)은 안티드론 시스템의 체계적인 구축을 위해 시스템 엔지니어링 절차와 디지털 트윈 기반의 모델링 및 시뮬레이션 도구를 활용한 검증 방안을 제시하였다. 본 연구는 안티드론 시스템의 설계, 개발, 시험 평가 단계에서 가상 시스템과 현실을 동기화하여 복잡한 전장 상황을 동일하게 구현할 수 있는 시뮬레이션 환경의 필요성을 강조하였다. 연구 결과, 디지털 트윈 기술 적용 분야를 장비 배치 및 성능 설정 평가, 제조사 및 통합 기관의 개발 시험, 시설별 요구성능 충족 여부 평가의 세 가지 분야로 구체화하여 제시하였다.[7]

정종운·이창한·이태명(2020)은 국회의 방호 취약성을 보완하기 위한 안티드론 방어체계 구축 방안을 제시하였다. 본 연구는 국회 보안 담당자와 안티드론 전문가를 대상으로 한 포커스 그룹 인터뷰와 해외 테러 사례 분석을 통해 다각적인 대응 전략을 도출하였다.

연구 결과 효과적인 방어체계 구축을 위한 방안은 원거리 탐지・추적・제압이 가능한 3지대 및 3선 방호개념 도입, 안티드론 전담 전문인력 확보 및 상황별 대응 메뉴얼 구축, 부수적 피해 최소화를 위한 법제도 정비와 영상 자료 기반의 증거 확보 절차 마련, 군・경 협력을 통한 통합방위태세 기반의 합동 대응체계 강화 등을 제시하였다.[8]

이와 같은 선행연구들을 종합하면, 국가중요시설을 대상으로 한 안티드론 시스템 구축 연구는 시설 등급별 대응 전략 도출, 드론 위협의 위험성 평가, 탐지 및 무력화 기술의 조합 등 기술적 토대로 마련하는 데 주력해 왔다. 특히 AHP를 활용한 영향 요인 분석, 드론 성능을 고려한 방호지대 설정, 정책・제도 개선 방향 제안 그리고 특정 시설의 현장 여건을 반영한 연구가 존재한다.

따라서 실제 발생 가능한 구체적 위협 시나리오를 따라 안티드론 시스템이 어떻게 설계・구성되어야 하는지에 대한 분석은 이제 실무적인 구축 단계를 향한 심화 논의가 필요한 시점이다. 즉 기존 연구들은 안티드론 시스템이 필요하다는 점을 충분히 답을 제시해 준 만큼, 이제는 “어떠한 위협이 발생할 때 어떠한 체계로 대응해야 하는가?” 라는 실증적인 구축 방안을 구체화해야 한다.

이에 본 연구는 단순히 표준화된 장비를 나열・배치하는 접근을 넘어 위협 유형별 맞춤형 방호 설계로 연구의 초점을 전환하고자 한다.

3. 연구 목적

방송시설은 국가 위기 상황에서 대국민 재난 경보와 사회적 안정을 담당하는 핵심 인프라이며, 주요국에서는 이를 국가중요시설로 지정・관리하고 있다. 그러나 그간 방송시설 보안은 담장, CCTV, 경비 인력 등 지상 기반의 물리적 침입 방어에 집중되어 왔으며, 최근 전쟁 사례에서 확인되듯 공중에서 접근하는 새로운 위협에는 충분히 대응하지 못하고 있다.

본 연구의 목적은 드론 위협이 증가하는 환경에서 방송시설이 직면한 구조적・제도적・기술적 한계를 분석하고, 국가중요시설로서의 특성을 반영한 실효적인 안티드론 대응 기반을 마련하는 데 있다. 방송시설은 공중에 노출된 자산이 많고 방송 연속성 유지라는 특수한 운영 조건을 갖고 있음에도, 드론 위협을 전제로 한 대응 기준과 절차에 대한 논의는

국내외에서 거의 이루어지지 않았다.

이에 본 연구는 방송시설의 자산 특성과 위협 유형을 체계적으로 분석하고, 위험분석기법을 기반으로 상황별 대응 전략을 도출함으로써 방송시설에 적합한 안티드론 시스템 구축 방법론을 제시하고자 한다. 이를 통해 향후 국가중요시설 전반에 적용 가능한 현실적인 대응 기준과 분석 틀을 마련하는 것을 목표로 한다.

4. 연구 범위 및 방법

가. 방송시설 안티드론 솔루션 구축을 위한 위험관리 프레임워크 수립

〔그림 1-7〕 방송시설 위험관리 프로세스

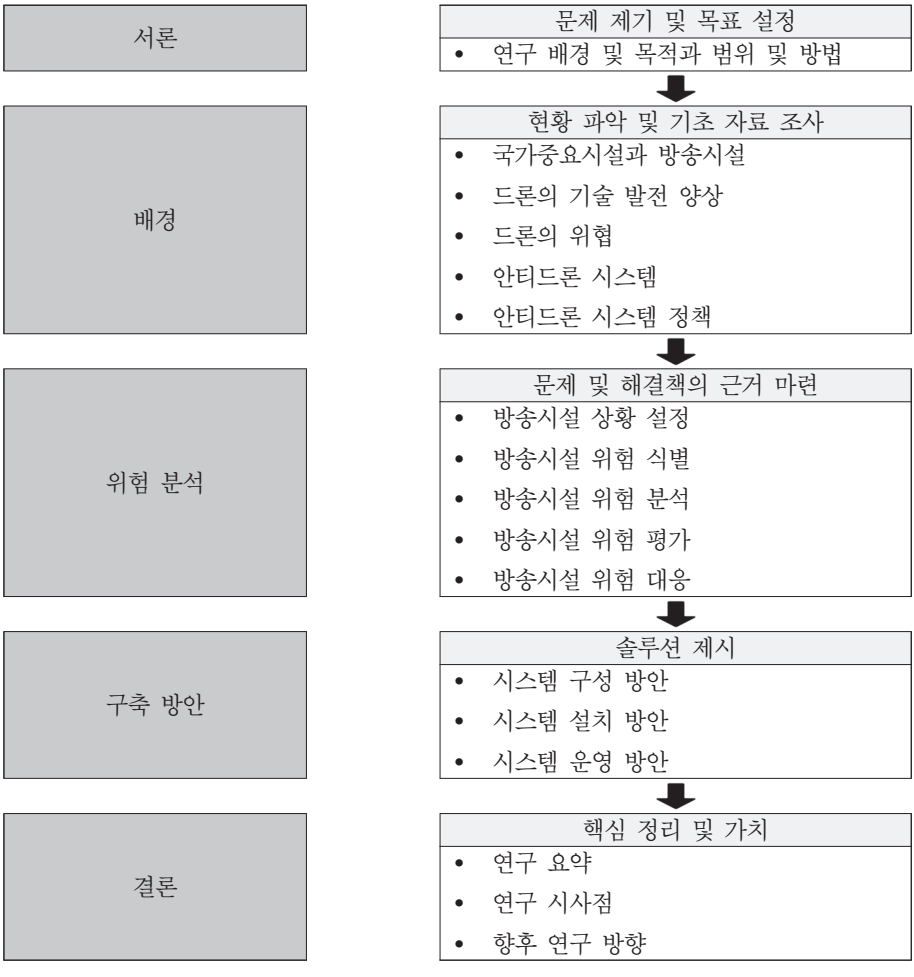
본 연구는 불법 드론 위협으로부터 국가중요시설인 방송시설의 안전성을 확보하고 최적의 방호체계를 구축하기 위해, 위험관리 국제 표준인 ISO/IEC 31000을 기반으로 분석 프레임워크를 수립하고, 세부 절차는 국내 표준 KS X ISO/IEC 27005를 준용하여 분석을 수행하였다. ISO/IEC 31000은 위험관리의 기본 프로세스를 제공하지만 세부 절차에는 한계가 있어, 정보보호 위험관리 표준인 KS X ISO/IEC 27005의 체계적인 절차를 방송시설 위험관리에 적용하였다.

국내외적으로 방송시설을 대상으로 한 안티드론 연구나 드론 위협에 대한 체계적인 위험 분석 사례는 매우 제한적이다. 이는 방송시설의 내부 자산과 잠재 위협 정보가 기밀로 관리되어 외부에서 전수 파악이 어렵기 때문이다. 이에 본 연구는 단일 기술을 제시하기보다, 시설 운영 주체가 직접 위협을 식별·평가하고 대응 방안을 도출할 수 있는 방법론

제시에 초점을 둔다.

본 연구에서 제안하는 프레임워크는 위협 환경과 운영 여건 변화에 따라 반복 적용이 가능한 순환적 평가 모델로 설계되었다. 이를 통해 실무자는 위험 분석 결과를 기반으로 안티드론 대응 전략과 구축 방향에 대한 합리적인 의사결정을 수행할 수 있다. 아래는 본 연구 수행의 흐름도이다.

〔그림 1-8〕 연구 수행 흐름도



나. 방송시설에서 드론 위협과 안티드론 운영 리스크의 통합적 위험 분석

본 연구에서는 방송시설에 가해지는 드론 테러 위협뿐만 아니라, 안티드론 시스템 운영 과정에서 발생할 수 있는 2차 위험을 동시에 분석이 요구된다. 방송시설의 특수성을 고려하여, 외부로부터의 드론 침투 위협과 이를 방어하는 과정에서 발생할 수 있는 안티드론 운영 리스크를 상호 연계하여 분석한다. 방송시설은 고출력 전파를 송출하는 국가중요기반시설로서, 단순한 방어 성공률뿐만 아니라 방송서비스의 연속성과 안전성이 동시에 보장되어야 한다. 따라서 두 가지 상충하는 위험 요소를 통합적으로 분석하여 최적의 균형점을 도출하는 것을 목적으로 한다.

다. 방송시설에서 실효적 운용을 위한 제도적·기술적 방안 연구

위험 평가의 선행 필수 조건으로서, 연구 대상 시설에 적용되는 국가 법령(항공안전법, 전파법, 테러방지법, 방송통신발전 기본법 등)에 대한 심층 분석을 수행한다. 방송시설은 도심 내 전파 밀집 지역에 위치하는 경우가 많아 기술적 차단뿐만 아니라 법적 제약이 강력하게 작용한다. 따라서 본 연구는 단순한 기술적 완성도를 넘어, 현행 법규 내에서 운용 가능한 안티드론 솔루션의 합법적 구축 방안을 모색하여 연구 결과의 현실 적용성을 확보한다.

4. 연구의 한계

본 연구는 통계적 분석 대신 공격 시나리오 기반의 분석 방식을 채택하였다. 이는 기존에 확인된 해외 테러 사례와 드론의 기술적 특성을 바탕으로 가상의 공격 상황을 설정하고, 그에 따른 피해 규모를 논리적으로 추론하는 방식이다. 전쟁 중인 국가를 제외하면 방송·통신 등 핵심 인프라를 직접적으로 타격한 사례에 대한 체계적인 통계 자료를 확보하기는 현실적으로 어렵다. 또한 이러한 위협은 일단 발생할 경우 사회적·국가적 파급 효과가 매우 크기 때문에, 제한된 정보 환경에서는 정량적 수치보다 최악의 상황을 가정한 정성적 분석이 불가피하다.

이에 본 연구는 실증 데이터 기반의 정량 분석에는 한계가 있음을 전제로 하되, 정보 부

재 상황에서 선제적인 대응책을 마련하기 위한 현실적이고 타당한 방법론으로서 시나리오 기반 분석을 적용하였다. 본 연구가 갖는 구체적인 한계는 다음과 같다.

1) 방송시설 정보자산 기밀성에 따른 자산 식별의 제한

방송시설은 국가중요시설로서, 핵심 송출 장비의 위치, 예비 전력 시스템, 상세 건축 도면 등이 기밀로 분류되어 외부 연구자의 접근이 원천적으로 차단된다. 따라서 본 연구는 외부에서 관측 가능한 시설 정보와 공개된 일반적인 방송 시스템 구조에 의존하여 자산을 식별하였다. 이로 인해 시설 내부에 은폐된 중요 자산이나 구체적인 취약점을 100% 정확하게 반영하지 못하는 '입력 데이터의 불완전성' 이 존재하며, 이는 최종 위험 분석 결과 및 구축 방안이 실제 조직의 내부 상황과 미세한 괴리를 보일 수 있다.

2) 정량적 위협 데이터의 부재

위험 분석에서 정량적 데이터란 과거의 사고 통계를 기반으로 미래의 위험을 확률적으로 계산한다. 그러나 안티드론 분야는 신생 위협으로, 국내 방송시설을 대상으로 한 드론 침투 횟수, 공격 성공률, 실제 폭발물 탑재 드론의 타격 피해액 등에 대한 누적된 과거 데이터가 전무하다. "방송시설에 드론이 연간 몇 회 출몰하는가?", "그중 몇 대가 공격형 드론인가?" 에 대한 정량적 모집단(Population)이 형성되어 있지 않기 때문에, 확률(Probability)을 적용한 수치적 위험 산출이 불가능하다는 통계적 한계가 존재한다.

3) 내부 전문가 부재에 따른 정성적 분석의 한계

통상 위험 분석을 위한 정성적 분석에서 델파이(Delphi) 기법 등 전문가 설문을 수행한다. 그러나 현재 대다수의 방송 시설 보안 조직은 지상 침입 방어에 특화되어 있어, 드론 위협에 대한 인식조차 저조한 상황에서 내부 실무자를 대상으로 한 설문이나 인터뷰는 유효한 데이터를 도출하는 데 한계가 있다. 즉, 숙련된 패널(Expert Panel) 확보의 어려움으로 인해, 현장을 반영한 정교한 정성적 평가 반영의 한계가 존재한다.

제2장 배 경

제1절 국가중요시설과 방송시설 정의

1. 국가중요시설

가. 국가중요시설의 개념

국가중요시설이란 「통합방위법」 제2조에 따라 공공기관, 공항·항만, 주요 산업시설 등 적에 의하여 점령되거나 파괴되거나 또는 그 기능이 마비될 경우[8] 국가안보와 국민 생활에 심각한 영향을 주게 되는 시설을 의미한다. 이러한 시설은 국가의 핵심 기능을 유지하는 기반으로 평시뿐만 아니라 비상사태 및 전시 상황에서도 안정적인 운영이 보장되어야 하는 전략적 중요 자산이다.

나. 국가중요시설의 대상

국가중요시설의 대상은「통합방위법」 제21조 제4항에 따라 국방부 장관이 관계 행정기관의 장 및 국가정보원장과 협의하여 지정한다[9]. 동 조항에 따른 국가중요시설 지정 체계는 시설의 물리적 형태나 소관 기관에 따른 단순 분류가 아니라, 국가 통치·행정 기능 유지, 에너지·산업·방송·정보통신·교통 등 국가기간 인프라의 안정적 운영, 재난 및 안보 대응과의 연계성 등 국가 운영 연속성에 대한 기여도를 종합적으로 고려하여 보호 대상과 보호 수준을 결정하도록 설계되어 있다.

특히 방송시설은 국가 통치·행정 기능 유지 및 재난 대응체계와 직접적으로 연계된 국가기간 기반시설로서, 재난·비상 상황에서 국민에 대한 신속한 정보 전달과 공공안전 유지에 필수적인 역할을 수행한다는 점에서 국가중요시설 지정 체계가 전제하는 보호 대상 범주에 포함되는 기능적 특성을 가진다.

---

8) 통합방위법 제2조 13호 [시행 2025. 10. 1.]

9) 통합방위법 제21조 제4항 [시행 2025. 10. 1.]

2. 방송시설

가. 방송시설의 정의와 역할

「방송통신발전 기본법」 제2조에 따르면, 방송통신시설이란 방송 및 통신을 수행하기 위하여 사용되는 기계·기구·선로 및 그 밖에 필요한 방송통신설비 일체를 의미한다. 이 중 방송시설은 방송통신시설 가운데 「방송법」에 따라 방송프로그램의 송출을 목적으로 설치·운영되는 시설을 말한다. 방송시설은 평시에는 방송프로그램의 안정적 송출을 통해 정치·경제·사회·문화 전반에 관한 정보를 국민에게 제공함으로써, 사회 전반의 정보 전달과 공적 의사소통이 원활히 이루어지도록 하는 핵심적인 공공 인프라로 기능한다.

방송시설은 재난 및 비상상황에서 재난방송, 행동 요령 안내, 정부 대응 조치 전달 등의 기능을 수행하도록 관련 법령[10]에 의해 운용된다. 「재난 및 안전관리 기본법」에 따라 방송시설은 재난 발생 시 방송을 통한 정보 전달이 주요 수단으로 활용되기 때문에, 방송시설의 기능 저하는 정부와 국민의 소통 수단이 단절됨으로써 사회 전체를 통제 불능의 대혼란으로 몰아넣는 심각한 국가적 위기로 직결될 수 있다.

〔그림 2-1〕 방송시설의 구성요소

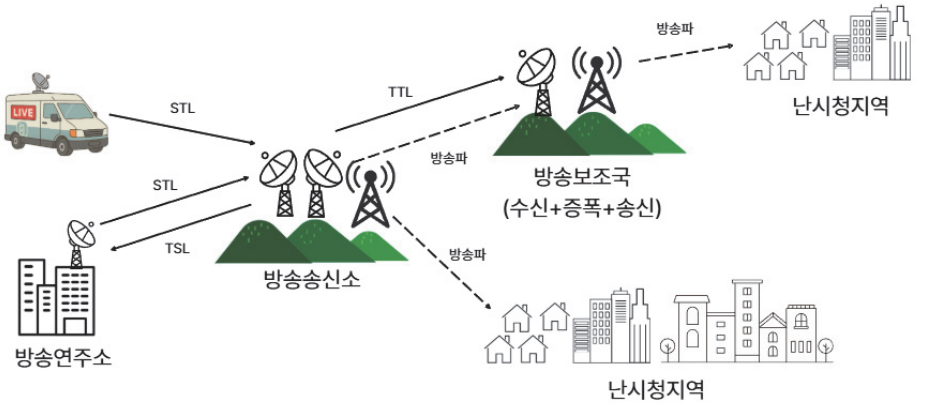
10) 방송통신발전 기본법 제35조 [시행 2025. 10. 1.]

나. 방송서비스

방송서비스란 방송사업자가 방송시설을 기반으로 제공하는 방송콘텐츠의 편성·전송 및 시청 행위 전반을 의미한다. 이는 시청자에게 제공되는 정보·오락·교육·문화 콘텐츠 자체와 그 전달 행위를 포함하는 개념으로, 지상파방송, 종합유선방송, 위성방송, 인터넷멀티미디어방송(IPTV) 등 다양한 형태로 제공된다. 본 연구에서는 방송서비스 전반을 포괄적으로 다루기보다는, 공공성 및 재난 대응 측면에서 가장 핵심적인 역할을 수행하는 지상파 방송시설을 연구 범위로 한정하여 분석한다.

다. 지상파 방송시설 구조

〔그림 2-2〕 지상파 방송시설의 구조



자료: 월간 방송과기술 중 “지상파 방송은 어떠한 경로로 전달되는가?” 재구성

지상파 방송전송의 구조는 방송국 등에서 제작한 프로그램을 가정에서 전달받기까지 여러 시설을 거치게 되며, 기능과 역할에 따라 연주소, 송신소, 방송보조국으로 구성된다[10]. 각 방송시설은 방송파와 방송링크로 구성되어 있으며, 방송링크는 방송사고 예방 차원에서 유선과 무선을 모두 사용하는 이중화로 설계되어 있다.

1) 방송연주소

방송연주소는 조정실과 스튜디오 등을 포함한 방송프로그램을 제작하는 곳이다. 이후 연주소에서는 영상과 음성등 방송콘텐츠를 제작하며 제작된 방송 신호는 마이크로웨이브 또는 광케이블과 같은 전송 수단을 통해 송신소로 전달된다.

2) 방송송신소

방송송신소는 연주소로부터 전달받은 신호를 수신받아 방송서비스 지역에 방송 신호를 전달하거나, 송신소/방송보조국으로 재송신하는 역할을 한다. 송신소 간 마이크로웨이브 전송망을 TTL(Transmitter to Transmitter Link)라고 한다.

2) 방송보조국

방송보조국은 난시청지역을 해소하기 위해 설치되는 시설로, 인근 송신소로부터 수신한 방송 전파를 다시 소출력으로 증폭하여 송신하는 '증폭 송신 방식'과, 송신소로부터 마이크로웨이브(TTL)를 전달받아 소출력으로 '재송신 방식'이 있다.

라. 지상파 방송시설 장비

1) 송신 철탑

송신 철탑은 안테나를 높은 고도에 지지하기 위한 핵심 구조물로, 전파 도달 거리를 확보하기 위해 설치된다. 철탑은 종류에 따라 지선식과 사각 자립식 철탑이 있으며, 고출력 중파 및 단파방송 송신소는 지선식을, 마이크로웨이브와 FM, DMB, TV 방송용 철탑은 자립식을 사용한다. 송신 철탑의 예시는 [그림 2-3]과 같다. 철탑은 모두 용융아연으로 도금된 고강도 철강을 사용하고 기초 풍속 및 하중을 고려한 설계로 철탑 구조 자체는 견고하다.

연주소 및 송신소의 철탑에는 통신 및 방송을 위한 안테나 여러 개가 설치되는 형태로 구성된다. 철탑들은 모두 고지대에 위치하며 사방이 트여 있어 드론의 3차원 접근 경로가 무제한으로 열려 있다. 또한 철탑에 거치된 케이블 트레이나 연결 부위는 소형 폭발물 드론의 타격에 취약할 수 있으며, 특히 지선식 철탑의 경우 드론을 이용해 '지선(Guy

wire)’ 연결 부위를 타격하거나 절단할 경우 구조물 전체가 붕괴될 가능성도 있다.

〔그림 2-3〕 철탑 구조 예시 - 자립식(왼), 지선식(오)

자료: 남강엔지니어링

2) 안테나

① 지상파 방송 안테나

지상파 방송용 안테나는 AM/FM 라디오, VHF(DMB), UHF(HD, UHD) 주파수 대역으로 구분된다. 송신용 안테나의 종류는 모노폴, 다이폴, 슈퍼턴스타일, 판넬형태가 있다. 지상파 방송 안테나의 종류와 그 모습은 <표 2-1>과 [그림 2-4]와 같다.

〈표 2-1〉 지상파 방송 안테나

방송대역	SW 라디오	AM 라디오	FM 라디오	DTV 방송	DMB 방송
안테나편파	수평	수평	원형	수평	수직
안테나 형태	모노폴		다이폴	패널, 슈퍼턴스타일	

〔그림 2-4〕 지상파 방송 안테나 예시

자료: WIKIPEDIA, WIKIMEDIA COMMONS 등

② STL 안테나

STL(Studio-to-Transmitter Link), TSL 안테나는 초지향성이므로, 가시선(LOS)가 필수적으로 확보되어야 한다. DTV 링크의 경우 M/W(마이크로웨이브) 링크에 사용되는 파라볼릭 안테나를 사용하며, 레이돔이 덮여있는 경우가 많다. FM 링크는 중장거리의 경우 1.7GHz 대역의 그리드 파라볼릭 안테나를 사용하며, 단거리 보조로서 야기(yagi) 형태를 사용한다. STL용 안테나는 [그림 2-5], [그림 2-6]과 같이 연주소 및 송신소 철탑과 중계차에도 설치된다.

〔그림 2-5〕 STL 안테나 예시

자료: WIRELESSUNITS, Broadcasters General Store, wiki1

〔그림 2-6〕 중계차에 설치된 STL 안테나 예시

자료: LRT mini DSNG. TVC - UAB TVC Solutions

3) 장비

① 방송 송신기 (Transmitter) 시스템

〔그림 2-7〕 방송 송신기 시스템 예시

자료: KBS OPEN BLOG 2014.03.20

[그림 2-7]은 방송 송신 시스템의 예시로 연주소에서 보내온 영상, 음성 등이 포함된 방송프로그램을 송신기에서 높은 출력으로 증폭하여 송신 안테나로 보내는 시설이다. 송신 설비는 변조기, 증폭기, 급전선, 안테나, 냉각기 등으로 구성된다. 여기서 송신기는 영상신호를 무선신호로 변환하는 변조기(Modulator)와 익사이터(Exciter)를 여러 개 결합한 고출력 증폭기(HPA), 고조파 제거 필터(Harmonic Filter)로 구성되어 전송된다.

② 방송 무선링크 (STL) 시스템

방송국 스튜디오에서 제작된 프로그램을 원격지의 송신소(산 정상 등)로 보내기 위한 무선 전송 시스템으로, 방송 신호를 무선주파수로 변환하여 송출 지점까지 안정적으로 전달하는 장비를 일컫는다. 일반적으로 링크 장비와 안테나만으로 구성이 가능하나, 전송 거리에 따라 RF 신호를 증폭 장비가 추가 구성된다. [그림 2-8]는 대표적인 방송 무선링크 시스템의 예시이다.

〔그림 2-8〕 방송 무선링크 시스템 예시

오디오용 디지털 송신기 링크

비디오용 디지털 M/W 링크 시스템

자료: SONIFEX AUSTRALIA 제품 등

링크 장비는 베이스밴드 신호를 마이크로파 등 무선신호로 변조하여 송신소로 전송하는 역할로, 오디오용 링크 장비는 일반적으로 오디오 인코딩 기능이 내장되어 있으나, 비디오는 별도 장비를 이용한다. 또한 수신부는 -95 dBm 정도의 매우 예민한 수신 감도를 가지고 있다. 또한 페이드마진(Fade Margin)이 20 dB~30 dB 이상으로 정상적인 설치 시 넉넉한 마진을 확보할 수 있는 시스템이다. 장비가 정상 수신하려면, 신호가 노이즈 플로어보다 최소한 일정 높이 이상 올라와 있어야 되는데, 이 C/N비가 22dB 이다.[32]

제2절 드론의 기술 발전 양상

1. 드론의 개념 및 종류

가. 드론 개요

드론은 조종자가 탑승하지 않은 상태에서 무선전파를 이용해 원격으로 조종되거나 사전에 입력된 프로그램에 따라 자동 또는 자율적으로 비행할 수 있는 무인항공기를 의미한다.[11] 「항공안전법 시행규칙」에서는 드론을 초경량비행장치의 한 유형인 무인비행장치로 분류하고 있으며, 기체 중량과 운용 목적에 따라 신고·비행 승인 등 관리 기준을 차등 적용하고 있다.[12] 드론은 소형·경량 기체부터 비교적 중량이 큰 기체까지 다양한 형태로 개발·운용되고 있으며, 카메라, 센서, 통신시스템 등 다양한 탑재체를 장착할 수 있다.

나. 드론 정의 및 용어

국내에서는 「항공안전법」을 통해 드론을 '초경량비행장'로 분류하며, 「항공안전법」 제2조에서는 초경량비행장치를 항공기 및 경량항공기 외에 공기의 반작용으로 비행할 수 있는 장치로 정의하고 있다.[13] 이후 드론 활용 범위의 확대에 따라 2020년 5월부터 시행된 「드론 활용의 촉진 및 기반 조성에 관한 법률」에 따라 '조종자가 탑승하지 아니한 상태로 향행할 수 있는 비행체'로 정의하고, 그 범위를 무인비행장치, 무인항공기뿐만 아니라 '원격·자동·자율 방식으로 항행하는 비행체'까지 포함하도록 개념을 확장했다.

본 연구에서는 용어 혼재로 인한 해석상의 혼선을 최소화하기 위해, <표 2-2>에 제시된 정의를 종합적으로 검토한 뒤 이에 해당하는 무인비행체를 포괄적으로 '드론'으로 통칭하여 사용한다.

---

11) 드론 활용의 촉진 및 기반 조성에 관한 법률 시행규칙 제2조 [시행 2025 3. 27.]

12) 항공안전법 시행규칙 [시행 2025. 12. 5.]

13) 항공안전법 제2조 [시행 2025. 11. 28.]

〈표 2-2〉 드론의 다양한 표현과 정의

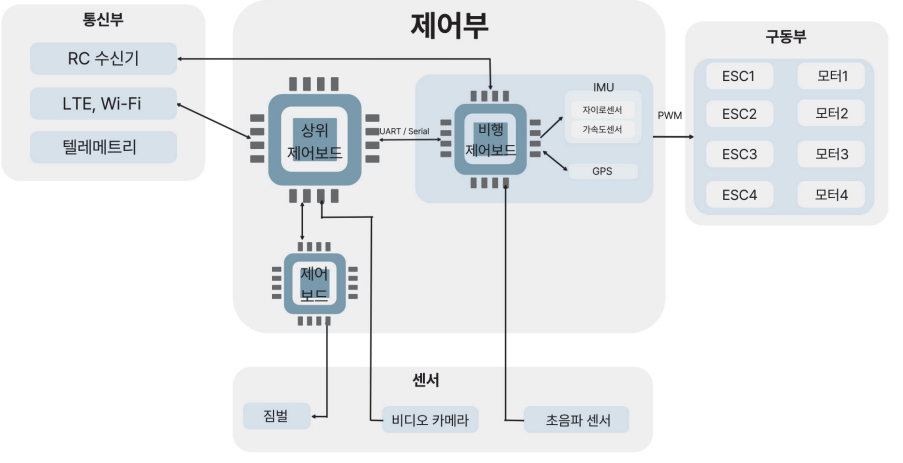
분 류	정 의
무인기 (무인기 시스템)	조종사가 비행체에 직접 탑승하지 않고 지상에서 원격조정, 사전 프로그램 경로에 따라 자동 또는 반자동 형식으로 자율비행하거나 인공지능을 탑재하여 자체 환경판단에 따라 임무를 수행하는 비행체와 지상통제장비 및 통신장비, 지원장비 등의 전체 시스템을 통칭
드론 (Drone)	사전 입력된 프로그램에 따라 비행하는 무인 비행체
RPV	Remote Piloted Vehicle 지상에서 무선통신 원격조종으로 비행하는 무인 비행체
UAV	Unmanned Aerial Vehicle 항공기에 탑승하는 조종사 없이 비행하는 항공기
UAS	Unmanned Aircraft System 무인기가 일정하게 정해진 공역뿐만 아니라 민간 공역에 진입하게 됨에 따라 Vehicle이 아닌 Aircraft로서의 안전성을 확보하는 항공기임을 강조하는 용어
RPAV	Remote Piloted Air/Aerial Vehicle 2011년 이후 유럽을 중심으로 새로 쓰이기 시작한 용어
Robot Aircraft	지상의 로봇 시스템과 같은 개념에서 비행하는 로봇 의미로 사용되는 용어

자료: 드론시장 및 산업동향(2017, 융합연구정책센터)[11]

다. 드론 구조

드론은 비행 제어부, 추진부, 통신부, 센서부 및 페이로드로 구성된 복합 시스템이다. 비행 제어부는 비행제어기를 중심으로 자이로센서, 가속도센서, 지자기센서, GNSS 수신기 등의 상태 측정 장치로부터 기체의 자세・위치・속도 정보를 수집・처리하여 비행을 제어한다. 추진부는 전자속도제어기(ESC), 모터, 프로펠러로 구성되며, 비행 제어부로부터 전달되는 PWM 신호에 따라 추력을 발생시켜 기체의 이동과 자세 제어를 수행한다. 통신부는 조종기 송・수신기, 텔레메트리 및 영상 송신 장치, 선택적으로 LTE 또는 Wi-Fi 통신 모듈을 포함하여 조종 신호와 비행・영상 데이터를 지상과 실시간으로 송수신한다. 센서 및 페이로드부에는 EO/IR 카메라, LiDAR, 레이다, 영상 센서 등 다양한 임무 장비가 탑재되어 감시・정찰・측정 등의 기능을 수행하며 모든 구성요소는 전원 공급 장치를 통해 통합적으로 운용된다. 전체적인 드론의 내부 구성은 [그림 2-9]과 같다.

〔그림 2-9〕 드론 구성도



자료: “회전익형 드론의 시스템 구성” 참고하여 재구성

라. 드론의 비행 방식에 따른 종류와 활용

〈표 2-3〉 비행 방식(양력 생성)에 따른 드론의 종류

구 분	구조	특성
고정익형	 고정된 날개를 통해 양력을 발생	장시간 비행 고속 비행
회전익형	 로터의 회전을 통해 양력을 발생	정지 비행 수직 이착륙
틸트로터형 (VTOL)	 고정익과 회전익의 혼합형태	구조가 복잡

드론은 비행 방식 및 구동 구조에 따라 <표 2-3>와 같이 고정익형, 회전익형, 틸트로터형으로 구분된다[13]. 이러한 분류는 드론의 비행 특성, 운용 환경, 활용 목적에 따라 기체의 구조적 차이를 달리해 활용한다. 특히 중소형 크기의 드론은 대부분 회전익 구조를 사용하며, 이는 수직 이착륙이 가능하여 공간 관계없이 이착륙이 가능한 이유가 가장 크다.

이러한 장점으로 인해 중소형 드론은 [그림 2-10]과 같이 민간영역과 군사·안보 영역에서 다양한 용도로 사용되고 있다. 민간·상용 영역에서는 촬영, 지도 제작, 농약 살포, 물류·경비 등 효율성과 편의성 향상을 목적으로 드론이 폭넓게 활용되고 있으며, 비교적 개방적 환경에서 산업·서비스 수단으로 정착하고 있다. 반면 군사·안보 영역에서는 정찰, 폭탄 투하, 자폭 공격, 보급 및 무기 운반 등 직접적인 위협 행위 또는 전술적 목적을 중심으로 드론이 활용되고 있으며, 동일한 중소형 기체라 하더라도 운용 목적과 사용 맥락에 따라 위험성이 현저히 달라진다.

〔그림 2-10〕 중소형 드론의 다양항 활용 예시

자료: 연합뉴스, 여수넷통뉴스 등

2. 드론의 기술 동향

가. 드론의 형태적 변화

1) 운용 영역 확장

최근 드론 기술은 공중 운용 중심에서 벗어나 지상・수상・수중 등 다양한 플랫폼으로 확장되는 다중 영역 통합 운용 양상을 보이고 있다. 공중 드론(UAV) 외에도 지상 드론(UGV)은 시설 내부 이동 및 정찰 임무에 활용[14]되고 있으며, 수상 드론(USV)은 항만・댐・연안 지역에서 운용[15] 사례가 증가하고 있다. 또한 수중 드론(UUV)은 해저 지형 조사 및 수중 기반시설 점검 등 목적으로 활용[16]되고 있다. [그림 2-11]는 지상, 수상, 수중 드론의 예시를 보여준다.

〔그림 2-11〕 지상・수상・수중 드론의 예시

지상 드론(UGV)

수상 드론(USV)

수중 드론(UUV)

자료: 네이트 뉴스, 지오소나, 로봇신문

2) 초소형화

드론 기술은 고효율 배터리와 모터 기술의 발전에 힘입어, 기존의 비행 성능을 유지하면서도 기체의 크기는 획기적으로 줄어드는 형태로 발전하고 있다. 드론을 초소형화하는 이유는 <표 2-4>와 같이 민간 영역과 군사 영역에서 그 목적성이 분명히 구분된다.

---

14) 지금은 지상 드론에 주목할 때, 드론매거진(Drone Magazine), 2024.05.07.

15) 댐 안전점검, 드론으로 꼼꼼히…소양강댐・안동댐 시범적용, The Science Times, 2020.06.19.

16) 수중 드론으로 독도 해저와 뱃길 해양환경 조사, 연합뉴스, 2017.02.24.

〈표 2-4〉 드론 초소형화의 목적

구 분	민간	군사
목적	사회적, 제도적, 물리적 제약 완화 대인 안전성	레이다 반사 면적 최소화 소음 최소화
설계 철학	“어디에서든 쓸 수 있게” “사람이 가까이에 있어도 쓸 수 있게” “사람에게 위화감이 없도록”	“안 들키고 임무를 완수하는가?”

최근 군사 분야에서는 [그림 2-12]과 같이 손톱 크기의 주사기형 드론부터, 수 그램(g) 단위의 소형 폭약만으로도 적의 지휘관이나 핵심 요인만을 선택적으로 제거할 수 있는 ‘초정밀 외과 수술식 타격(Surgical Strike)’ 수단으로 발전하고 있다.

〔그림 2-12〕 초정밀 외과 수술식 타격(Surgical Strike) 드론의 예시

자료: 중앙일보, nownews 등

나. 드론 통신 기술의 변화

2000년대 초반 디지털 통신 기술의 비약적 발전과 함께, 2010년대로 접어들며 2.4 GHz ISM(Industrial, Scientific, and Medical) 대역과 대역 확산(Spread Spectrum) 기술이 본격적으로 확산되었다. 이는 드론을 단순한 비행체에서 센서와 통신 기능을 결합한 '날아다니는 센서 플랫폼'으로 전환시키는 계기가 되었다. 드론 통신 기술은 기체 형상이나 비행 제어 기술의 발전보다도 장거리 운용과 은닉성을 중심으로 발전해 왔으며, 1950~2000년대의 72 MHz 기반 단순 제어를 거쳐 현재는 GHz 대역 광대역 무선통신을 통해 대용량 데이터를 실시간으로 전송하는 단계에 이르렀다. 더 나아가 전자전 환경에서의 생존을 위한 저피탐(LPI)·항재밍(Anti Jamming) 기술이 적용되고 있으며, 통신 거리의 한계를 극복하기 위해 위성 및 셀룰러 네트워크 기반 통신으로 확장되고 있다.

1) 드론 통신의 분류

<표 2-5>는 드론의 통신 기술을 특성에 따라 분류한 결과이다. 크게 무선과 유선으로 분류되며 드론 통신 기술의 선택은 임무의 목적(영상품질, 제어 거리, 보안)에 따라서 달라진다.

〈표 2-5〉 드론의 통신 기술 분류

구 분	무선				유선
	지상기반		비 지상기반(위성)		광섬유
	지상국	셀룰러	위성 제어형	GPS 기반 임무형	
핵심기술	전 주파수 대역 활용	LTE, 5G NR	LEO, GEO	GNSS	케이블 관리
지연시간	매우 낮음 (<10~20ms)	중간 (50~100ms)	매우 높음 (>600ms)	-	극히 낮음
통신 대역폭	낮음-높음	높음	낮음-높음	-	매우 높음
보안 및 간섭성	재밍에 취약	상용망 보안 의존	비교적 안전	완전 면역	완전 면역
통신 거리	수 km ~ 수십 km	셀 커버리지 의존	수백 km~ 수천 km	수백 km~ 수천 km	수백 m~ 수 km

2) 드론 민간 허가 주파수 대역

드론의 무선통신 시스템은 비행 제어(C2, Command & Control)와 영상・관측 정보를 포함한 임무 데이터 전송을 담당하는 핵심 인프라이다. 과거에는 FSK, DSSS, FHSS가 각각 독립적으로 적용되었으나, 최근 드론 통신 기술은 이들 방식을 결합하여 항재밍 성능과 전송 효율을 동시에 확보하는 방향으로 발전하고 있다. 드론 통신 주파수는 물리적 특성에 따라 제어용 Sub-1 GHz 대역과 영상・관측용 ISM 대역으로 구분되며, 2025년 기준 주요 국가별 허가 주파수 현황은 <표 2-6>과 같다.

〈표 2-6〉 2025 민간 드론 무선통신용 허가 주파수

미국		한국		유럽		일본	
제어	영상/관측	제어	영상/관측	제어	영상/관측	제어	영상/관측
433 MHz 1.2 GHz 2.4 GHz 5.8 GHz	915 MHz 1.2 GHz 2.4 GHz 5.8 GHz	917 MHz 2.4 GHz 5.8 GHz	917 MHz 2.4 GHz 5.8 GHz	433 MHz 868 MHz	2.4 GHz 5.8 GHz	73 MHz 920 MHz 2.4 GHz 5.8 GHz	169 MHz 1.2 GHz 2.4 GHz 5.8 GHz

자료: 미국 FCC, 한국 MSIT, 유럽 CEPT/ETSI, 일본 MIC/TELEC 참고

최근에는 상용 주파수를 사용하는 드론은 전자전 장비에 탐지 및 무력화되기 쉬워 비표준/불법 주파수를 사용하기도 한다. ELRS(ExpressLRS) 오픈소스가 이를 가속화 시켰으며, RF 트랜시버 칩[17]이 지원하는 주파수 대역이 포함되는 경우, 소프트웨어 설정(레지스터 값 등)만 바꾸면 어디든 쏠 수 있기 때문에 이러한 변칙적인 주파수 사용이 쉽게 가능해졌다. <표 2-7>은 대표적인 RF 트랜시버 칩과 사용 가능한 주파수 대역을 보여준다.

17) 신호 송수신, 변조 기능을 하는 단일 반도체 소자(IC)

〈표 2-7〉 대표적 RF 트랜시버 칩의 주파수 대역

회 사	모델	허용 주파수	용도
Semtech	SX1276	137 MHz ~ 1020 MHz	LoRA
TI	CC1352	169~1050 MHz 2.4 GHz	IoT 제어
AD	AD9361	70 MHz ~ 6.0 GHz	SDR

자료: Semtech, TI, AD에서 제공하는 레퍼런스 매뉴얼 및 스펙 시트 참고

3) 지상국 기반 드론의 무선통신 기술

최근 드론 통신 프로토콜은 단순한 주파수 도약을 넘어, 전송 효율과 보안성을 동시에 확보하는 고대역폭 전송과 적응형 기술의 결합한 하이브리드 방식으로 발전하고 있다. 주요 기술적 특징은 <표 2-8>과 같다. 최근 지상국 기반 통신기술에서는 단순한 1:1 연결이 아니라, 드론과 드론, 지상국이 서로 거미줄처럼 연결되는 '모바일 애드혹 네트워크(MANET)'를 형성하여 최대 50km까지 작전 범위를 확대하는 기술로 발전하고 있다.

〈표 2-8〉 주요 드론 무선 데이터링크 기술 비교

프로토콜	변조	확산·보조 기법	주파수 대역	특징
DJI Ocusync Autel	QAM OFDM	Adaptive FHSS	2.4/5.8 GHz	고대역폭 영상 전송
Wifi	QAM OFDM	FHSS	900 MHz	범용성
Doodlelabs	QAM OFDM	MANET Radio	1.2 GHz 2.2-2.3 GHz (허가·전용)	메시네트워크기반 초장거리
TBS Crossfire	CSS	-	900 MHz	장거리
ImmersionRC Ghost	CSS	Adaptive FHSS	2.4 GHz	장거리 항재밍 성능 강화
Radio Link	QPSK BPSK	Legacy FHSS	2.4 GHz	레거시 기술을 활용 안정성 있는 통신
FRSKY ACCST	FSK Legacy FHSS	Legacy FHSS	2.4 GHz	

자료: DJI, Doodlelabs, TBS 등 제조사 공개 기술 자료 및 제품 설명을 바탕으로 작성

제3절 드론의 위협

1. 드론 위협의 개념

가. 일반 테러

드론 테러의 개념을 규명하기에 앞서 먼저 일반적인 테러의 개념을 살펴볼 필요가 있다. 국내에서 테러에 대한 법적 정의는 「국민보호와 공공안전을 위한 테러방지법」 제2조에 명시되어 있으며 동 법에 따르면 테러란 국가·지방자치단체 또는 외국 정부의 권한 행사를 방해하거나 의무 없는 일을 하게 할 목적, 공중을 협박할 목적으로 사람, 항공기, 선박 시설 등을 대상으로 공격·방해·파괴·조작·폭파 등의 불법적인 행위[18]를 말하며 구체적인 테러의 정의와 범위를 <표 2-9>과 같이 정의하고 있다.

〈표 2-9〉 테러의 정의

구분	내용
사람	사람을 살해하거나 사람의 신체를 상해하여 생명에 대한 위험을 발생하게 하는 행위
항공기 및 항공시설	운항 중인 항공기를 추락시키거나 전복·파괴하는 행위, 그 밖에 항공기의 안전을 해칠 만한 손괴를 가하는 행위
선박 또는 해상구조물	운항 중인 선박 또는 해상구조물을 파괴하거나 안전을 위태롭게 할 정도의 손상을 가하는 행위
생화학·폭발성·소이성 무기 또는 장치의 활용	기차·전차·자동차 등 공중이 이용하는 차량 및 관련 시설에 배치하거나 폭발시키는 행위
핵물질 및 방사성물질	원자로를 파괴하여 공공의 안전을 위태롭게 하는 행위

자료: 「국민보호와 공공안전을 위한 테러방지법」 제2조

나. 드론 테러

1) 드론 테러의 정의

18) 국민보호와 공공안전을 위한 테러방지법 제2조 [시행 2024. 2. 9.]

드론 테러는 조종자가 탑승하지 않은 무인 비행체를 활용하여 공중에서 앞서 정의한 테러의 정의를 수행하는 행위이다[15]. 드론은 기존의 어떠한 위협보다 인명이나 주요시설에 직접적인 물리적 피해를 쉽게 가할 수 있을 뿐만 아니라 감시・정찰・교란, 위험 물질이나 물품의 운반 등 다양한 방식으로 공공 안전과 국가 기능에 심각한 영향을 미칠 수 있다.

2) 의도성에 따른 드론 위협 행위의 분류

위협 행위 목적과 의도에 따라 크게 비의도적 위협과 의도적 위협으로 구분된다. 비의도적 위협은 테러의 목적은 없으나, 조종자의 부주의, 조종 미숙, 기체 결함, 통신 두절 등으로 인해 발생하는 우발적 사고를 의미한다. 반대로 의도적 행위는 명확한 악의적 목적을 가지고 수행되는 행위이다. 폭발물 탑재를 통한 직접 타격, 불법 물품 반입, 시설 무단 침입 및 정찰, 사이버 해킹 중계 등 계획된 테러 행위가 이에 해당한다. 이에 대해서 드론의 위협 유형과 이에 따른 특징 및 예상 피해를 <표 2－10>에 정리하였다.

〈표 2－10〉 드론의 위협 유형 세부 분류

구분	주요 행위 및 특징	예상 피해
비의도적	조종자 과실	시설물 충돌 및 파손 항공기 운항 지연 및 회항 단순 사생활 침해 분쟁
	기체 및 장비 결함	낙하로 인한 인명 상해 중요시설 기능 일시 마비 2차 안전사고 유발
의도적	감시 및 정찰	군사/국가 보안 기밀 유출 테러 실행을 위한 사전 정보 노출 심각한 프라이버시 침해
	물품 밀반입	범죄 악용 및 기초 질서 붕괴 위험 물질 유입으로 인한 안전 위협
	직접 타격	대규모 인명 살상 핵심 기반시설 파괴 사회적 공포 및 혼란 조장
	방해	항공기의 의도적 방해
	전자전 및 사이버전	내부 전산망 침투 및 정보 탈취

다. 드론 관련 법과 제도

1) 드론 실명제와 드론 자격증

드론으로 인한 테러를 사전 예방과 안전사고 예방하기 위해 2021년 3월 「항공안전법」 시행규칙을 개정하여 드론 실명제(기체 신고제)와 조종 자격 차등화 제도를 도입하였다. 기존에는 자체 중량 12kg을 초과하는 기체만 신고 대상이었으나, 제도가 강화되면서 2kg 이상을 초과하는 드론이면 신고가 의무화되었다. 드론의 신고를 하지 않고 비행할 경우 500만 원 이하의 벌금에 처해지며[19], 위반으로 최대 200만 원의 과태료도 부과된다. 이러한 제도는 제도권 내의 드론을 식별하고 관리하는 최소한의 안전장치로 작동하고 있으나, 실질적인 단속이 되지 않다. 드론 조종에 대한 자격제는 2025년 현재 <표 2-11>과 같다.

〈표 2-11〉 드론 조종 자격증 제도

자격구분	비행장치 무게	취득요건	비고
1종	25kg 초과 ~ 150kg 이하	비행경력 20시간 이상	농업용 대형 방제 드론
2종	7kg 초과 25kg 이하	비행경력 10시간 이상	중형 촬영 드론
3종	2kg 초과 ~ 7kg 이하	비행경력 6시간 이상	일반 취미드론
4종	250g 초과 ~ 2kg 이하	온라인 교육 이수	
대상 아님	250g 이하	-	

자료: KDEC 한국드론교육센터

2) 드론 비행금지구역

국토교통부는 「항공안전법」에 따라 국가안보와 항공기 안전을 위해 드론 비행금지구역을 지정하고 있으며, 해당 구역에서의 비행은 관할 기관의 사전 승인이 필요하고 무단 비행 시 300만 원 이하의 과태료가 부과된다. 또한 DJI 등의 주요 드론 제조사들은 GPS 기반의 소프트웨어 제한을 적용하고 있으나, 이는 펌웨어 해킹이나 자작 드론에 대해서는 실효성이 제한적이다.

19) 항공안정법 제161조 제3항 [시행 2025.12.30.]

〔그림 2-13〕 드론 비행 금지(빨간 빗금) 및 제한 구역(초록 빗금)

자료: BBS News (2024.06.)

[그림 2-13]은 드론 비행이 원칙적으로 금지되는 구역과 조건부로 제한되는 구역을 구분하여 나타낸 것이다. 빨간 빗금으로 표시된 구역은 항공안전 및 국가·공공시설 보호를 위해 드론 비행이 전면 금지되는 지역이며, 초록 빗금으로 표시된 구역은 사전 승인이나 조건부 허가가 있을 경우에 한해 제한적으로 비행이 가능한 구역을 의미한다.

3) 주요 불법 운용 시 법적 책임 및 처벌

드론의 불법 운용은 단순한 항공법 위반을 넘어, 국가안보 침해, 사생활 침해, 밀수 및 테러 등 다양한 범죄 유형으로 확장될 수 있다. 특히 드론은 원격·비대면 운용이 가능하다는 특성으로 인해 행위자의 신원 은폐가 용이하며, 동일한 기체라도 운용 목적과 행위 방식에 따라 행정 처분 수준의 위반에서 중대 범죄에 이르기까지 법적 책임의 범위가 크게 달라진다. 이에 따라 드론 관련 불법 행위는 항공안전법을 비롯하여 군사기지법, 군사

기밀보호법, 형법, 성폭력처벌법, 마약류관리법, 항공보안법 등 개별 법률에 따라 처벌되며, 일부 행위는 무기징역이나 사형까지 적용될 수 있는 중범죄로 분류된다. 이러한 드론 불법 운용 유형별 적용 법률과 처벌 수위는 <표 2-12>과 같다.

〈표 2-12〉 드론 불법 운용 유형별 적용 법률 및 처벌 수준

위반유형	구체적 행위	적용 법률	최대 처벌 수위
단순 침입 (의도/비의도)	비행금지구역 미승인 비행	항공안전법	과태료 300만 원
	야간비행 위반		과태료 200만 원
안보 위협 (스파이/정찰)	군사기지 시설 무단 촬영	군사기지법	징역 3년 3,000만 원
	군사 기밀 탐지 및 수집 행위	군사기밀보호법	징역 10년
사생활 침해 (범죄 악용)	성적 수치심 유발 신체 촬영	성폭력처벌법	징역 7년 벌금 5,000만 원
	주거 침입 및 무단 촬영	형법(주거침입)	징역 3년 500만 원
	동의 없는 영상촬영	개인정보보호법	징역 5년 5,000만 원
밀수 (마약/물품 반입)	마약 등 의약품 밀반입	마약류관리법	무기징역
	교도소 등 금지 시설 내 물품 투하	형법(업무방해)	징역 2년 벌금 2천만 원
테러 (의도적 가해)	항공기 납치・점거・파괴	항공보안법	사형 및 무기징역
	인명 살해・상해	형법(살인 및 상해)	
	주요시설 폭파	형법(건조물 폭발)	
		형법(폭발물사용)	

자료: 국가법령정보센터

2. 국내외 드론 위협 사례 및 처벌

가. 국외

1) (비의도적 침입) 백악관 드론 충돌

2015년 1월 26일, 직경 약 61cm 규모의 소형 상업용 드론 1대가 미국 백악관 건물 남동쪽 구역에 충돌하는 사건[20]이 발생하였다. 약 6시간 뒤 드론 소유자가 자발적으로 연락하여 조사받은 결과 해당 사고는 취미용 드론 조종 중 발생한 실수로 확인되어 테러 목적은

없는 것으로 결론을 내리고 형사 기소는 하지 않았다. 하지만 이후 미국의 본격적인 드론에 대한 위협을 자각한 사례가 되었다. [그림 2-14]는 실제 백악관에 떨어진 소형 드론의 모습이다.

〔그림 2-14〕 백악관 내에 떨어진 소형 드론

자료: 한국일보

2) (의도적 가해) 일본 총리 관저 드론 테러

2015년 4월 22일, 일본 도쿄 총리 관저 옥상에서 미량의 방사성 물질이 담긴 소형 드론이 발견되는 사건[21]이 발생하였으며, 이후 원전 재가동 반대를 주장한 야마모토 야스오가 경찰에 자수하였다. 조사 결과 야마모토는 같은 달 9일, 총리 관저에서 서쪽으로 약 200m 떨어진 주차장에서 드론을 띄워 관저 방향으로 비행시켰고, 드론에 부착된 플라스틱 용기에는 후쿠시마 귀환 곤란 지역에서 채취한 흙과 원전 반대 성명문이 담겨 있던 것으로 확인되었다. 해당 드론은 10일 이상 관저 옥상에 방치된 상태로 있다가 4월 22일에야 직원에 의해 발견되었으며, 범행에 사용된 기체는 중국 DJI사의 팬텀 모델로 일반인이 쉽게 구매할 수 있는 상업용 드론이었다. 일본 검찰은 야마모토에게 '위계에 의한 업무방해' 혐

20) '드론'에 혼쭐 난 백악관…가장 막기 힘든 공격수단, SBS 뉴스, 2015.01.28.

21) '원전 반대' 일본 40대 남성, '총리관저 드론' 자수, 한겨레, 2015.04.26.

의 등을 적용하여 기소하였고, 징역 2년에 집행유예 4년을 선고하였다. [그림 2-15]은 실제 일본 총리 관저의 모습과 침입한 드론의 모습을 보여준다.

〔그림 2-15〕 일본 총리의 관저에 침입한 드론

자료: 조선일보

3) (의도적 가해) 베네수엘라 대통령 테러

2018년 8월 4일 베네수엘라 수도 카라카스에서 열린 국가방위군 창설 81주년 기념행사 도중 니콜라스 마두로 대통령을 겨냥한 드론 테러 사건[22]이 발생하였다. 대통령이 연단에서 연설을 진행하던 중 폭발물을 탑재한 드론 여러 대가 공중에서 연쇄적으로 폭발하였으며 이로 인해 행사장은 큰 혼란에 빠졌다. 테러에 사용된 드론은 중국 DJI사의 산업용 기종으로 약 1kg의 C-4 플라스틱 폭약이 적재된 것으로 확인되었다. 폭발은 대통령이 위치한 연단 인근과 주변 건물 상공에서 발생하였으나 암살 시도는 실패로 끝났고 그 과정에서 군인 7명이 부상을 입었다. 베네수엘라 당국은 사건 직후 용의자 6명을 체포하였으며, 단순한 시위나 소요 사태가 아닌, 국가 원수 살해를 목적으로 한 반역 행위이자 테러로 규정하였다. 사건 발생 4년 뒤인 2022년 8월, 법원은 전직 야당 의원인 후안 레케센스를 포함한 주동자 및 가담자 17명에게 최고 30년에서 5년의 징역형을 선고하였다.

22) 베네수엘라 대통령, '드론 폭탄' 테러 피습…배후는 누구?, 글로벌이코노믹, 2018.08.05.

〔그림 2-16〕 베네수엘라 대통령 폭탄드론 암살 미수사건

자료: 경향신문

나. 국내

1) (의도적 침입) 고리원전 드론 침입

〔그림 2-17〕 고리 원자력 발전소 불법 드론 적발

자료: KBS 뉴스

2019년 8월, 1급 국가보안시설인 고리원자력발전소 상공에서 이틀 연속 드론으로 추정되는 비행체가 출현했으나, 군·경의 감시에도 실체와 운용자를 특정하지 못한 채 사건은 종결되었다.[23] 이 사건은 국내에서 국가중요시설을 대상으로 한 드론 위협을 본격적으로 인식하는 계기가 되었다. 이후 원전 주변 드론 비행 사례가 이어지고 있으나, 조종자 신원이 확인되더라도 항공안전법 위반에 따른 최대 200만 원 과태료에 그쳐 대응과 처벌의 한계가 지적되고 있다.[24]

〈표 2－13〉 2024년 원안위 드론 침입건수 보고

구분	2020	2021	2022	2023	2024
	4(4)	3(3)	139(48)	106(65)	144(84)
장비 도입 여부	도입 이전			도입 이후	
합계	252(120) 약 55%			281(178) 58%	

주) 탐지건수는 조종자 확인 건수를 나타냄
자료: 원자력안전위원회

2) (의도적 침입) 인천공항 활주로 드론 침입 및 회항

2020년 9월 인천국제공항 인근에 불법 드론이 출현해 항공기 5대가 김포국제공항으로 회항하고, 활주로 운영이 약 1시간 중단되는 사건이 발생했다.[25] 경찰은 CCTV 분석 등을 통해 드론 조종자 2명을 적발했으나, 항공안전법 위반으로 각각 200만 원의 과태료만 부과했다. 2025년 기준 최근 5년간 불법 드론의 공항침입 사례는 비행금지구역 위반 669건, 관제권 위반 289건으로 기록되며, 부과된 과태료만 16억 원에 달한다[26]. 이러한 사례들은 항공보안법 적용 요건을 고려할 수 있으나, 테러·의도적 침해로 처벌된 사례가 없다. 따라서 현재 모두 항공안전법 위반으로 처리된 것으로 보인다.

23) 고리원전 상공에 이틀 연속 드론 추정 비행체 출현… 군·경, 실체 규명도 없이 사건 종결, 조선일보, 2019.08.16.
24) 원전 '드론출현' 속출 "처벌 낮아, 재밍기술 활용해야", 뉴시스, 2019.10.07.
25) 인천공항에 뜬 불법 드론..항공기 5대 회항 소동, SBS 뉴스, 2020.09.26.
26) 불법드론 적발, 5년간 1166건 과태료 15억7000만원, 뉴시스, 2025.10.07.

〔그림 2－18〕 인천국제공항 회항 사건(왼쪽)과 4년간 운항 피해(오른쪽)

자료: SBS 뉴스

3) (안보 위협) 중국인의 국정원 무단 촬영

2024년 6월, 서울 서초구 내곡동 국가정보원(NIS) 청사 인근에서 중국 국적 남성이 드론으로 청사를 무단 촬영하다 적발되는 사건이 발생했다. 해당 인물은 유네스코 세계문화유산인 헌인릉 촬영 과정에서 우연히 건물이 촬영되었다고 주장했으며, 경찰은 항공안전법 및 군사기지 및 군사시설 보호법 위반으로 구속 송치했으나, 명확한 대공 혐의가 입증되지 않아 석방하였다. 이 사건은 드론 촬영 이후 '실수'를 주장할 경우 간첩죄 등 중대 범죄 적용이 어렵다는 법적 한계를 보여주는 사례로 평가된다.

〔그림 2－19〕 국정원 불법 촬영 사건

자료: MBN 뉴스

제4절 안티드론 시스템

1. 안티드론 개념

앞서 살펴본 바와 같이 드론 기술은 형태의 다양화와 통신 방식의 고도화를 중심으로 발전하고 있으며, 이에 따라 활용 범위 또한 지속적으로 확대되고 있다. 이러한 기술 발전은 산업·공공 분야에서의 활용성을 높이는 한편, 불법 비행, 무단 촬영, 감시·정찰, 테러 등 공공의 안전과 질서를 위협하는 행위에 악용될 가능성도 함께 증가시키고 있다. 특히 자율비행 기능의 상용화와 초소형 기체의 확산은 기존의 물리적·전파 중심 보안체계만으로는 드론 위협을 사전에 탐지하거나 통제하는 데 한계를 발생시키고 있으며, 이는 개인의 생명·신체·재산 보호뿐 아니라 국가 기능의 안정적 유지 측면에서도 새로운 위험 요소로 작용하고 있다.

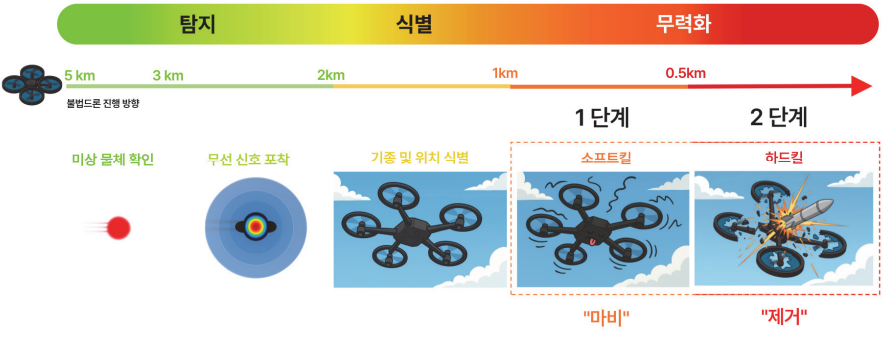
이러한 기술 환경 변화에 따라 위협 드론은 운용 형태, 통신 방식, 기체 규모, 자율성 수준 등에 따라 다양하게 분류되며, 유형별로 탐지 가능성과 대응 방식에서 상이한 특성을 보인다. 초소형·자율비행·유선 드론 등은 시각·레이다 탐지나 전파 교란 기반 대응의 효과가 제한적이어서, 단일 센서나 단일 수단만으로는 효과적인 대응에 한계가 있다. 이에 따라 공공의 안전과 질서를 확보하기 위해서는 위협 특성에 맞춘 탐지·식별·대응 수단을 연계·통합한 체계적인 안티드론 시스템 구축이 요구된다.

가. 안티드론 시스템 정의

안티드론 시스템은 드론 테러에 대비하기 위한 개념으로 '안티드론', '드론 방호' 등 다양한 용어로 사용되고 있으며 해외에서는 일반적으로 C-UAS(Counter Unmanned Aerial System)로 국내에서는 '안티드론 시스템'이라는 명칭으로 통용되고 있다[2]. 안티드론 시스템이란 드론을 이용한 불법 침투, 무단 촬영, 테러 행위(폭발물, 위협물 탑재등)와 같은 위협을 탐지하고 식별한 후 무력화를 통해 안전을 확보하는 것을 목적으로 한다.

안티드론 시스템은 센서를 활용한 탐지·식별 기술과 물리력에 따른 비행 무력화 기술로 구성되며 [그림 2-21]과 같이 기존 군의 공중방위 개념인 '공중감시-식별-요격'을 드론의 영역으로 가져와 '탐지-식별-무력화'라는 3단계로 규정하고 있다[17].

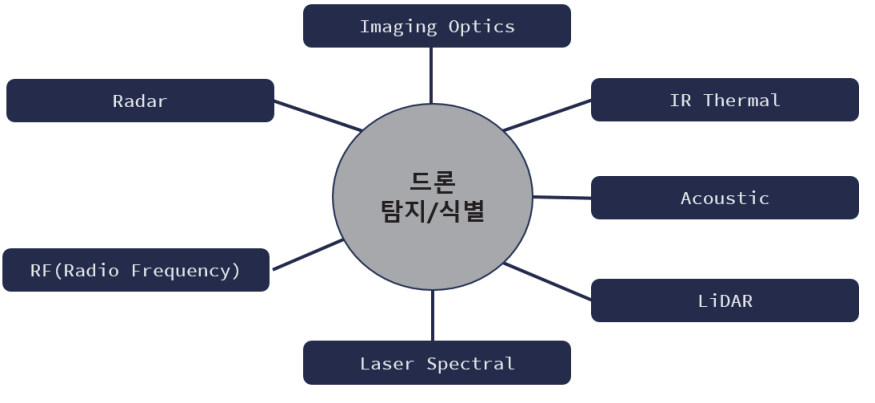
〔그림 2-20〕 안티드론 시스템의 구성



이 시스템은 방호 영역에 접근한 초소형 비행체를 탐지한 뒤, 이를 드론인지 다른 물체인지 구분하고, 위협 드론으로 판단될 경우 무력화를 통해 위험을 제거하는 것이 기본적인 운용 개념이다. 최근에는 기체 소형화로 인해 피탐지율이 낮고 위치 정밀도가 높은 드론의 등장으로 이에 대응하기 위한 안티드론 기술의 정밀성과 정확성이 더욱 중요해지고 있으며 미국, 이스라엘, 중국, 유럽 등 주요 국가를 중심으로 국가 정책 연구와 방산·레이다 산업을 기반으로 관련 기술개발이 이루어지고 있다[15].

나. 안티 드론 시스템 : 탐지 및 식별

〔그림 2-21〕 드론 탐지/식별을 위한 주요 센서 기술



1) 탐지 : 레이다(Radar) 센서

〔그림 2-22〕 드론 탐지 장비의 예시 - 레이다

자료: EDR Magazine 2022.06.15, 뉴스 드림 2024.01.18

레이다는 전자파를 방사한 후 표적으로부터 반사되어 돌아오는 신호를 수신하여 표적의 존재를 탐지[18]하고 전파의 왕복 시간을 분석함으로써 표적까지의 거리와 위치를 산출하는 센서이다. 최근 드론 특성을 고려한 AESA 레이다[27] 가 있다. 레이다는 초소형 물체에 대한 오인식이나 사각지대 발생 가능성, 높은 가격이라는 한계를 내포하고 있음에도, 탐지 범위가 다른 센서에 비해 넓어 드론 탐지 체계에서 배제할 수 없는 센서로 인식되고 있다.

2) 탐지 및 식별 : RF 센서

〔그림 2-23〕 드론 탐지 장비의 예시 - RF 스캐너

자료: Dedrone, AARONIA AG

27) KF-21 AESA 레이다(능동형 위상 배열 레이다)

RF 센서는 드론 운용 시 송수신되는 무선주파수 신호를 감지하여 드론의 존재를 탐지하고 식별하는 기술이다[18]. 대부분의 상용 드론은 특정 주파수 대역을 이용해 조종기와 통신하므로 드론에서 방출되는 RF 신호를 탐지하면 신호의 정보를 기반으로 드론의 방향과 기종을 식별한다. 최근에는 탐지만 머물지 않고 신호를 복조하여 해석 후 드론을 식별하는 기술까지 적용되어 상용화되어, 현재는 가장 가성비가 뛰어난 센서로 인식되고 있다.

3) 탐지 : 음향 센서

〔그림 2-24〕 드론 탐지 장비의 예시 - 음향 탐지

자료: Aviation Week Network 2018.04.26.

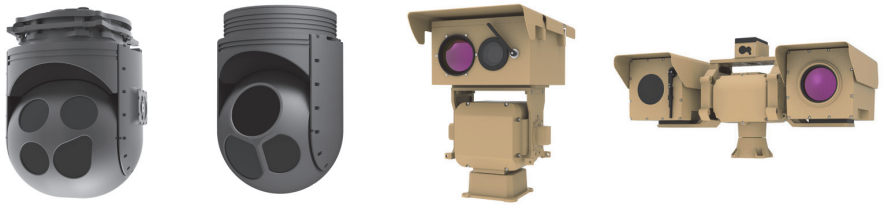
음향 탐지 센서는 드론 비행 시 모터와 프로펠러에서 발생하는 고유의 음향 신호를 감지하여 드론의 존재를 탐지하는 센서이다. 탐지된 소리가 드론에서 발생한 음향인지를 판단하기 위해서는 다양한 드론 기종별 음향 특성을 사전에 데이터베이스화하고 이를 기반으로 비교・분석하는 과정이 필요하다[15]. 가격이 낮고 운용이 간편하나 주변 환경 소음에 민감하여 성능이 제한된다. 최근에는 광섬유 드론으로 인해 다시 각광받고 있다.

4) 탐지 및 식별 : 영상(Electro Optic/Infrared) 센서

영상 센서는 가시광선(Electro Optic) 및 적외선(Infrared) 영역의 영상을 획득・처리하여 표적을 탐지하고 식별하는 기술로 안티드론 시스템에서 시각적 확인 수단으로 활용된다.

EO 센서는 드론의 색상, 외형, 크기, 비행 시 모터와 전자 장치에서 발생하는 열 신호를 감지함으로써 조류 등 자연 물체와의 식별에 효과적이다. AI 기반으로 비약적으로 발전하였으나, 여전히 영상 기반 탐지는 광학적 특성과 센서 해상도에 의해 탐지 거리와 범위에 한계가 있으며 단독 운용 시에는 표적의 정확한 위치 파악이 어렵다는 제약이 있다[19].

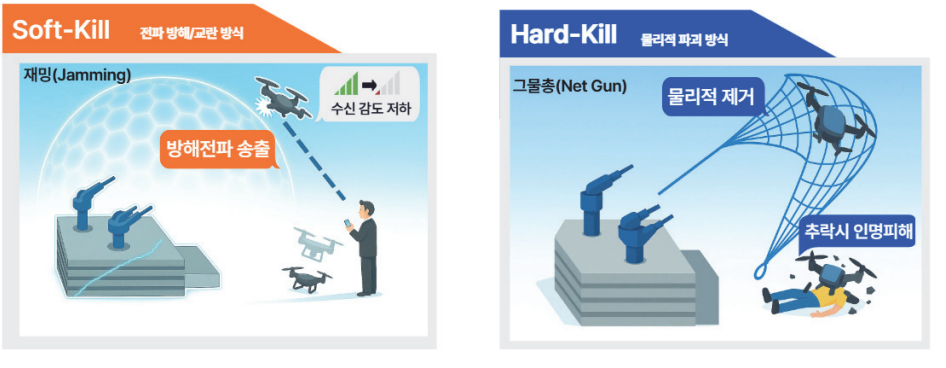
〔그림 2-25〕 드론 탐지 장비의 예시 - EO/IR 카메라



자료: TBT SYSTEM

다. 안티드론 시스템 : 무력화

〔그림 2-26〕 소프트킬(왼쪽) 방식과 하드킬(오른쪽) 방식의 차이



드론 무력화 기술은 위협으로 판단된 드론의 임무 수행 능력을 상실시키거나 비행을 중단시키는 것을 목적으로 하며 운용 방식에 따라 소프트킬(Soft-kill)과 하드킬(Hard-kill) 방식으로 구분되고, 소프트킬 방식은 단순 소프트킬과 정밀 소프트킬 두 가지 방식으로 구분된다. 소프트킬 방식은 신호 차단 등을 통해 드론의 통신 또는 항법 기능을 마비시키는 비물리적 대응 방식이며, 하드킬 방식은 드론 기체를 직접 파괴하거나 강제로 추락시키는 물리적 대응 방식이다[20]. 이러한 무력화 기술은 보호 대상 시설의 특성, 주변 환경, 법적·제도적 제약을 종합적으로 고려하여 선택·운용되어야 하며 안티드론 시스템의 실질적인 방호 성능을 결정하는 수단이다[5].

〔그림 2-27〕 소프트킬 장비와 하드킬 장비의 예시

자료: 담스테크, D-Fend, 카이든 등 제품

이와 같이 드론 무력화 기술은 적용 방식과 효과 범위에 따라 다양한 기술로 세분화되며, 각 기술은 대응 범위, 정밀도, 부작용 및 법적 제약 측면에서 서로 다른 특성을 가진다. 따라서 실제 대응체계에서는 단일 기술에 의존하기보다 보호 대상과 운용 환경에 적합한 기술을 선택 및 조합하여 접근하는 것이 요구되며, 드론 무력화 기술의 유형별 주요 특성은 <표 2-14>와 같다.

〈표 2－14〉 무력화 기술의 유형별 특성

유형	종류		설명	장점	단점
하드킬	레이저		고출력 레이저로 드론 센서 또는 기체 손상 유발	원거리 정밀 조준 가능, 탄약 소모 없음	악천후 영향 고위험
	HPM		고출력 마이크로파로 전자회로 기능 상실 유도	다수 드론 동시 영향 가능	전자장비 파괴
	그물		발사형 그물로 드론 포획	기체 회수 가능	근거리만 대응 고속 드론 불가
	요격 드론		요격 드론이 직접 접근하여 파괴 또는 포획	기동성 우수, 특정 표적 대응 가능	다수드론 한계
소프트킬	단순	방사형 재밍	광역 전파 방출로 통신 차단	넓은 범위 통제 가능	타 통신 간섭 지속적 대응 한계
		재밍건 및 지향성 재밍	특정 방향 전파 방해	주변 영향 최소화	타 통신 간섭 지속적 대응 한계
		GPS 스푸핑	위성항법(GNSS) 신호 기만	기체 손상 없이 무력화 가능	IMU, 비전 등 혼합센서 기반 기동 드론 불가
	정밀	스마트 재밍	선택적 주파수/시간 방해	불필요한 전파 간섭 감소	고도화된 분석 기술 필요
		제어권 탈취형	제어권 탈취 후 강제 착륙 또는 유도	통제된 무력화 가능	

자료: 안티드론(Anti-Drone) 정책 발전 방안, Robotic Warfare 다가오는 무인화 전쟁의 시대 참고하여 재구성

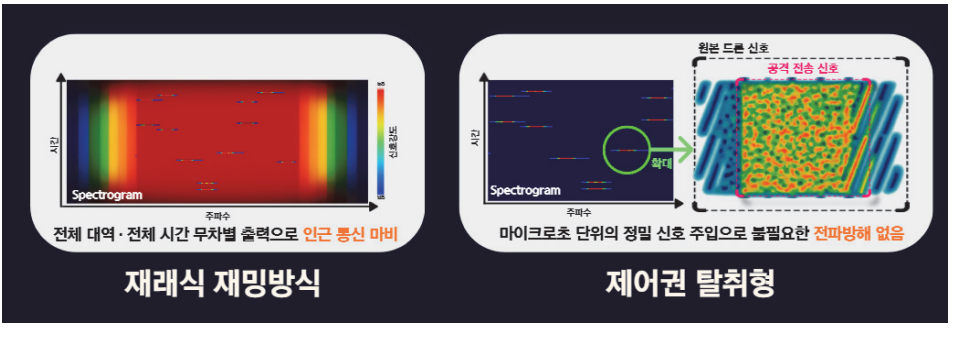
이해를 돕기 위해 이하에서는 단순 및 정밀 소프트킬 방식과, 전자기적·물리적 파괴를 수반하는 하드킬 방식의 주요 기술과 특성을 예시 중심으로 살펴본다.

1) 단순 소프트킬 : 전파 교란

단순 소프트킬은 드론과 조종기 간의 무선 통신을 대상으로 주파수 교란(Jamming)을 수행하여 드론의 정상적인 비행을 방해하는 방식이다. 드론이 사용하는 제어 신호(C2) 또는 영상·데이터 링크 대역에 강한 전파를 방사함으로써 통신 품질을 저하시켜, 드론이 비행을 지속할 수 없도록 하거나 사전에 설정된 페일세이프(Fail-safe) 동작을 유도한다. 일반적으로 통신 두절 시 드론은 자동 착륙, 호버링 후 추락, 또는 이륙 지점으로의 귀환(RTH) 등의 동작을 수행하게 된다. 이로 인해 단순 소프트킬은 신속한 위협 차단 수단으로 활용되거나 군집 드론에 대응 목적으로 활용되기에 용이하다.

2) 정밀 소프트킬 : 제어권 탈취

〔그림 2-28〕 단순 소프트킬(왼쪽)과 정밀 소프트킬(오른쪽)의 차이



제어권 탈취 기술은 단순히 주파수를 교란(Jamming)하여 드론의 비행을 방해하는 것을 넘어, 드론과 조종기 간의 통신프로토콜을 분석하거나 위조된 신호를 정확한 타이밍과 주파수에 송신하여 드론의 제어 권한을 강제로 확보하는 방식이다. [그림 2-28]은 단순 소프트킬과 정밀 소프트킬의 차이를 시각적으로 나타낸다. 드론이 사용하는 통신 주파수 대

역의 프로토콜을 실시간으로 분석하여, 공격자가 마치 정당한 조종자인 것처럼 위장한 신호를 드론에 전송하여, 위협 드론을 안전한 구역으로 강제 착륙(Safe Land)시키거나 이륙 지점으로 강제 귀환시킬 수 있는 기술이다. 단점으로는 모든 드론이 가능한 것은 아니며, 현재 기술로는 미식별 프로토콜을 사용하는 커스텀 드론에 대해서는 대응이 제한될 수 있다. 현재 가장 진보된 소프트킬 기술로서 전파방해 없이 민간에서도 활용할 수 있는 안티 드론 무력화 기술로서 인식되고 있다. 이스라엘과 미국에서 상용화에 성공하여, 현재 미국 및 유럽등 민간영역에서 운용 중이다.

3) 하드킬 : HPM

〔그림 2-29〕 HPM 장비의 예시

자료: FUTURO PROSSIMO

HPM(고출력 마이크로파) 기술은 지향성 에너지를 사용하여 드론의 전자 부품을 영구적으로 손상시키거나 오작동을 유발하는 전자기적 하드킬 방식이다. 고출력의 마이크로파 펄스를 목표 드론을 향해 방사한다. 강력한 전자기파는 드론의 안테나나 틈새를 통해 내부로 침투하여 전자 회로와 센서에 과전류를 유발, 반도체 칩을 태우거나 시스템을 셧다운 시킨다. 레이저나 총탄이 1:1 요격에 특화된 것과 달리, HPM은 넓은 빔 폭을 가지고 있어 다수의 드론이 동시에 공격해오는 군집 드론 공격을 일시에 무력화하는 데 매우 효과

적이나, 유효사거리가 상대적으로 짧고, 주변 장비에 심각한 피해를 일으킬 수 있다. 최근에는 빔포밍 방식으로 적 드론과 아군 드론을 구별하여 무력화할 수 있다. 미국, 러시아에서 상용화에 성공하여 군사 영역에서 운용 중이다.

2. 국내외 안티드론 시스템 구축 사례

가. 국외 사례

1) 미국

〔그림 2-30〕 사일런트 아처 대드론 시스템

자료: Arm Technology

미국은 초기에는 기존 방공 레이다 체계를 활용하여 드론 위협에 대응해 왔으나 드론의 소형화・저고도화가 진행됨에 따라 기존 방공 시스템만으로는 효과적인 대응에 한계가 있다는 인식이 확산되었다. 이에 따라 미국은 레이다 기반 탐지를 중심으로 하되 레이다 탐지가 어려운 소형 드론에 대해서는 전자추적 시스템과 광학 카메라를 결합한 별도의 안티드론 체계를 도입・운용하고 있다. 미 육군은 2017년 약 720억 원 규모의 안티드론 시스템

을 도입한 데 이어 2019년에는 약 1,200억 원 규모의 추가 구매 계약을 체결하였으며 공군 역시 약 630억 원 규모의 안티드론 시스템을 도입하였다. 실제 운용 결과 안티드론 시스템 도입 이후 다수의 드론 공격이 단기간 내 급격히 감소하는 효과를 보였다. 다만 장거리, 중간 및 단거리 탐지와 무력화 기능을 통합한 시스템은 구축 비용이 높고 운용 난이도가 커 숙련된 전문인력이 필수적이라는 한계를 지니고 있다.[28]

2) 영국

〔그림 2-31〕 영국 개트윅 공항 활주로의 안티드론 시스템

자료: 아주대학교 국방디지털융합학과[29]

영국은 2018년 12월 개트윅 공항 인근에서 발생한 드론 출몰 사건을 계기로 안티드론 대응의 필요성을 본격적으로 인식하게 되었다. 당시 드론 침입으로 인해 약 1천 편 이상의 항공편이 결항되고 14만 명 이상의 이용객이 불편을 겪는 등 사회·경제적 피해가 발생하

28) US Army awards $108m anti-drone technology contract to SRC, Army Technology, 2019.01.31.

29) 英공항 '드론 사태' 일단락..이스라엘 드론 돔이 해냈다, 중앙일보, 2018.12.23.

였다. 이후 2019년 히드로 공항에서도 유사한 사건이 발생하면서 드론 위협이 항공안전에 실질적인 위험 요소로 부각되었다. 이에 영국 정부는 이스라엘 라파엘사가 개발한 '드론 돔' 시스템을 군용으로 도입하여 운용하고 있으며 공항 보호를 위해 탐지 장비와 함께 그물 발사 방식의 무력화 장비 도입도 추진하고 있다.[30]

3) 프랑스

〔그림 2-32〕 안티드론 소총

자료: CAMBIO

프랑스는 테러 위협에 대비하여 군 차원에서 안티드론 대응 능력을 체계적으로 강화하고 있다. 프랑스군은 별도의 지대공 방어 부대를 중심으로 안티드론 훈련을 실시하고 있으며 드론을 전자적으로 무력화할 수 있는 소총형 재머와 물리적 타격이 가능한 소총을 병행 운용하는 방식으로 대응체계를 구축하였다.[31]

30) 방해 전파 쏘고, 직접 격추까지… '안티 드론' 새롭게 부상, 조선일보, 2018.12.27.
31) ¡Tienes que verlo! Ejército francés experimenta con armas futurísticas, CAMBIO, 2019.07.15.

4) 일본

일본은 2015년 총리 관저 옥상에 방사성 물질을 담은 드론이 침입한 사건을 계기로 국가중요시설에 대한 드론 방호체계를 강화하였다. 일본 경시청은 드론 위협에 전문적으로 대응하기 위해 무인항공기 대처부대를 창설하고 국가중요시설과 비행금지구역을 중심으로 드론 침입 대응 임무를 수행하고 있다. 불법 드론이 접근할 경우 헬기를 통한 경고 방송을 실시하고, 이에 응하지 않을 경우 요격 드론을 출동시켜 그물 방식으로 불법 드론을 포획·무력화하는 체계를 운용하고 있다.[32][8]

나. 국내 사례

1) 평창 동계올림픽

〔그림 2-33〕 평창 동계올림픽 안티드론 시스템

자료: 조선일보

2018년 평창 동계올림픽 및 패럴림픽 개최 기간 동안 드론을 이용한 테러와 안전사고를

32) 일본 경찰 "무인기로 무인기 잡는다", 연합뉴스, 2015.12.08.

예방하기 위해 대회 조직위원회와 관계 기관은 경기 지역을 중심으로 총 4개 권역(1권역: 강릉권, 2권역:평창권, 3권역:봉평권, 4권역:정선권)으로 구분된 드론 통제 공격을 설정하고 엄격한 비행 제한 조치를 시행하였다. 아울러 올림픽 기간 동안 평창과 강을 상공에는 길이 약 17m의 전술용 유선 비행선을 띄어 150~200m 상공에서 24시간 감시·정찰 임무를 수행하도록 하였으며 야간 촬영이 가능한 고성능 카메라를 통해 확보된 영상은 조직위원회 안전관리실뿐만 아니라 대테러 업무를 담당하는 정부 기관에서도 실시간으로 공유되었다. 이와 함께 드론 위협에 대비한 다층적 대응체계도 운용되었는데 의심 드론이 탐지될 경우 우선 전파 차단 기술을 활용한 무력화를 시도하고, 필요시 전문 요원이 산탄총을 이용해 격추를 시도하는 방식으로 적용되었다.[33]

2) 인천국제공항

〔그림 2-34〕 인천국제공항 드론 탐지 시스템

자료: 보안뉴스

33) 軍비행선·킬러 드론 떴다… 테러 꼼짝마, 조선일보, 2018.01.10.

인천국제공항은 국내 민간공항 가운데 최초로 안티드론 탐지 시스템을 구축하여 2020년 9월부터 시범 운용을 실시하였다. 해당 시스템은 항공기의 안전 운항을 위협할 수 있는 불법 드론을 선제적으로 탐지하고 대응하는 것을 목적으로 하며 이를 위해 레이다 기반 탐지 기술과 주파수 탐지 방식을 적용하여 드론 탐지 정확도와 신뢰성을 높였으며, 시범 운용 결과를 바탕으로 시스템을 보완한 후 2021년 말부터 안티드론 탐지 시스템을 본격적으로 운영할 계획을 수립하였다. 그리고 불법 드론 탐지 시 포획 및 격추 등 실질적인 차단 조치를 신속히 수행하기 위해 민·군·경 간 협력체계를 강화하고 관련 기관과 업무협약 체결하여 통합 대응체계를 구축해 나갈 계획이다.[34]

34) 인천국제공항공사, 국내 민간 공항 최초로 드론탐지시스템 시범 운영 개시, 보안뉴스, 2020.11.20.

제5절 안티 드론 시스템 정책 및 법적 동향

국제 안보 환경 변화, 즉 전쟁에서 드론이 군사적으로 막대한 효용성을 발휘하는 사례는 군사 영역뿐만 아니라 민간영역에서도 드론 대응 기술 확보의 중요성을 부각시켰으며, 이에 따라 전 세계적으로 안티드론 시스템 구축이 진행되고 있다. 본 절에서는 안티드론 기술을 군과 민간 영역 모두에서 실전적으로 운용하기 위한 법적 근거와 정책적 추진현황에 대해 동향을 분석한다. 또한 해외의 법적, 정책적 사례를 바탕으로 국내 방향성을 미리 예측한다.

1. 국내 안티드론의 정책 및 법제 추진현황

가. 정책

국내 안티드론 정책은 국가안보, 국방, 교통・항공안전, 해양・항만보안 등 분야에서 드론 위협이 증가함에 따라 정부 부처를 중심으로 선제적 대응체계 구축이 본격적으로 추진되고 있다. 특히 국방부・합참, 국토교통부, 해양수산부가 각각의 관할 영역에서 안티드론 대응 정책을 우선적으로 도입하며, 국가 차원의 통합 대응 기반 마련을 위한 제도 정비와 기술개발을 병행하고 있다.

2019년 10월 정부는 선제적 규제 혁파 로드맵 제시에서 안티 드론 도입을 위한 제도 마련을 처음으로 밝혔다. 기존에는 불법 드론의 침입으로부터 국가 주요시설을 보호하기 위해 드론 전파차단 장비의 활용이 필요하나, 현행 법령에서는 불가능한 상황이었기에 전파법 등에서 금지하고 있는 재밍(전파차단) 장비 도입・운영을 위해 전파법 및 공항시설법을 개정 추진하겠다고 밝혔다.[35]

2020년 9월 국토교통부와 인천국제공항공사는 인천공항에 안티드론 시스템을 시범 도입하며 선제적 대응에 나섰으나, 주로 탐지 레이다와 RF 스캐너를 통한 모니터링 장비를 설치하였다. 물리적 무력화 수단인 ‘하드킬(Hard-kill)’이나 전파를 교란하는 ‘소프트킬

35) 드론 분야 선제적 규제혁파 로드맵 발표, 과학기술정보통신부, 2019.10.17.

(Soft-kill)’ 방식은 2019년 정부 로드맵 이후에도 법적 리스크로 인해 전면적인 운용이 여전히 불가하였다.[36]

2023년 2월 정부는 북한 무인기 침투 사건 이후 제16차 국가테러대책위원회를 개최하여 국가중요시설 안티드론 보완대책을 심의・의결했다. 정부는 국가중요시설에 대해 시설 중요도 등에 따른 우선순위를 선정하고 단계별로 도입 추진계획과 또한 관련 기술 연구개발(R&D)을 적극 추진하고 관련 법령과 제도도 개선계획을 밝혔다.[37]

2023년 3월 국민의힘 홍석준 의원은 전파차단장치 사용 기관의 손실보상 및 책임자에 대한 구상권 청구(선보상 후 구상권 청구) 관련 법적 근거를 담은 ‘전파법’ 개정안을 발의하였다. 즉 전파법 제29조에서 불법 드론을 방어하는 시스템의 사용을 허가됨에도 사용을 주저하는 문제점을 해결할 계획임을 밝혔다.[38]

2024년 01월 국토교통부는 안티드론 시스템이 구축되지 않은 울산, 여수, 무안, 양양 등 4개 민간공항은 2026년까지 안티드론 시스템을 구축하고 민군 겸용공항은 유관 기관과 함께 불법 드론, 무인기 등에 대한 대응체계를 올해 안에 구축할 계획을 밝혔다.[39]

2024년 10월 해양수산부는 무역항 안티드론 시스템을 위해 항만공사가 사업비를 50:50으로 분담하여 안티드론 구축사업에 착수할 예정이라 밝혔다. 2025년까지 안티드론 시스템 구축을 완료할 계획이라고 밝혔다.

나. 법제

국가중요시설 드론 방호 정책의 일환으로 대통령훈령 제398호「통합방위지침」제15조(국가 중요시설의 경비・보안 및 방호)를 기반으로 2021년 7월에는 국방부 훈령 제2575호「국가중요시설 지정 및 방호훈령」제12조(방호능력)를 개정하여, 기존 지상 위주의 2차원적인 방어체계로 구축되어 있어 드론과 같은 공중위협에 대응을 할 수 있도록 하였다.

---

36) 민간공항은 “26년까지 안티드론 시스템을 구축하고 민군 겸용공항은 관계기관과 대응체계를 갖출 계획입니다.”, 국토교통부, 2024.01.30.

37) 국가중요시설에 드론 테러 막는 ‘안티드론 시스템’ 단계적 도입, 정책브리핑, 2023.02.17.

38) “불법드론 막아라” 전파차단장치 손실보상 근거법 추진, 서울경제, 2023.03.21.

2022년 12월 북한 드론 침입 사태 이후 정부는 관련 법 개정안을 발의하기 시작했다. 발의되고 개정된 국내 안티드론 시스템과 관련된 법제는 크게 안티드론 시스템을 운용하는 권한 자체에 대한 법안 개정과 운용에 따른 책임 면책 법안의 개정이 독립적으로 발전하고 있다. 이는 권한만 있고 면책 조항이 없을 때 법을 개정하여 전파차단이나 포획 권한을 부여하더라도, 대응 과정에서 발생하는 2차 피해 책임을 전적으로 져야 한다면, 법의 실효성이 떨어지기 때문이다.

1) 안티드론 시스템 운용 권한 관련 법안 개정 동향

2020년 06월 「전파법」 제 29조 '혼신 등의 방지'를 대폭 수정하였다. 기존에는 비상통신을 제외하고는 혼신이나 그 밖의 방해를 절대 허용하지 않았었다. 하지만 드론 및 사제 폭발물 등에 따른 위협을 방어하기 위한 전파이용을 방해 또는 차단하는 장치를 사용할 수 있다고 명시하였다. 그리고 아래의 활동 또는 조치 등의 범위에서 전파차단장치를 사용할 수 있다고 명시하였다. 또한 통합방위작전 상황이 아니더라도, 공항 및 원자력시설에 한해서는 불법 드론이 출현했을 때 상시적으로 대응할 수 있는 법적 근거를 마련하였다.

1.「대통령 경호에 관한 법률」 제5조 제3항에 따른 안전활동
2.「통합방위법」, 「군사기지 및 군사시설 보호법」 등에 따른 국가안전보장 목적의 군사활동
3.「국민보호와 공공안전을 위한 테러방지법」 제2조 제6호에 따른 대테러활동
4.「공항시설법」 제56조 제7항에 따른 위반행위의 제지
5.「원자력시설 등의 방호 및 방사능 방재 대책법」 제2조 제1항 제3호에 따른 물리적방호

2024년 2월 국토교통부는 「공항시설법」 제56조 제3항 조항을 예외조항을 추가하여 불법 드론에 대한 활동 조치가 국가 및 지자체는 물론 공항운영자, 비행장시설을 관리·운영하는 자로 활동의 주체를 확대하고 무단으로 공항 주변에 접근하거나 침입하는 불법 드론

에 대한 조치가 가능하도록 강화되었다. 기존 법령에 따르면, 공항의 경우 공항시설법 제56조 제3항에 따라 제약을 받고 있어 누구든지 항공기, 경량항공기에 위험을 일으키는 행위는 불법으로 간주 되어, 불법 드론에 대한 대응 자체가 불가하였다. 현재는 불법 드론을 공항 근무자가 적극적으로 차단할 수 있는 근거를 마련되었다. 하지만 공항시설법 개정으로 대응 주체는 확대됐지만, 전파차단 등 전파이용을 직접 방해하는 장치의 사용 권한 자체가 명시적으로 부여된 것은 아니다.

2) 안티드론 시스템 운용에 따른 책임 면책 법안의 개정 동향

2024년 1월「공항시설법」 개정안 제56조의 3에 대한 예외조항이 신설되었다. 진압 과정에서 예상치 못하게 발생할 수 있는 제3자의 사상, 재산상의 피해에 대해 형사처벌 면책 및 손실보상 규정을 공항시설법에 신설하였다. 특히, 형사처벌 면책과 손실보상 규정을 동시에 신설한 첫 사례라고 볼 수 있다. 다만 이는 공항이라는 특정 시설과 조건에 한정된 특례적 법이다.

2024년 1월「전파법」 개정안 제29조의 2(면책)이 신설되었다. 「전파법」 제29조 제3항에 진압 과정에서 예상치 못하게 발생할 수 있는 제3자의 사상, 재산상의 피해에 대해 형사처벌 면책 및 손실보상 규정을 「전파법」에 신설하였다. 특히, 전파방해로 인한 형사처벌 면책과 손실보상 규정을 동시에 신설한 첫 사례다.

2024년 07월 「전파법 시행령」 제53조의 4 및 별표 5의 2를 신설하여, 전파차단장치 사용으로 인한 손실의 보상기준 및 보상절차를 마련하였다. 국내에서 전파법에 근거한 안티드론 체계에 대해 보상 구조를 구체화한 첫 사례다.

두 법안 개정안 모두 전파차단 기반 방어 수단이 잠재적 위험성과 부작용을 내포하고 있음에도 불구하고, 중대한 위협에 대응하기 위한 허용 가능한 수단으로 인식하고, 그 운용을 위한 법적 근거와 제도적 틀을 마련하려는 시도로 해석된다. 결과적으로 공공 목적하에 전파차단장치를 운용하는 경우, 그 운용 과정에서 발생할 수 있는 일정 수준의 위험을 국가가 제도적으로 흡수하겠다는 정책적 방향성을 시사하지만, 이러한 접근은 다음과 같은 한계를 동시에 내포하고 있다.

첫째, 기존 소프트킬 대응체계, 특히 전파차단 방식이 필연적으로 수반하는 통신 간섭 및 부수적 피해 가능성을 제도적으로 인정하였다.

둘째, 형사책임에 대해서는 별도의 면책 규정이나 특례 조항이 마련되었다고 보기 어렵다. 즉, 전파차단장치 운용과 관련된 형사책임은 여전히 기존 전파법, 통합방위법 등 형법 관련 법령에 따라 개별 사안별로 판단될 수밖에 없는 구조이다.

2. 국가중요시설 드론 방호 정책 및 법제의 실효성 한계

가. 도입 강제성 결여 및 운용 실효성 부재

현행 안티드론 관련 법령은 안티드론 장비의 사용 근거를 일부 시설에 한해 마련하는 데 초점이 맞춰져 있을 뿐, 국가중요시설이라 하더라도 드론 방호 장비의 도입 및 설치 의무를 명시적으로 규정하고 있지 않다. 설령 도입 의무가 부여된다 하더라도 미이행 시 이를 제재할 벌칙 규정이 부재하여, 현실적으로 시설 관리 주체의 이행을 강제할 동력이 부족하다.

또한, 공항과 원자력시설을 제외한 대다수 국가중요시설(방송국 등)은 전파차단장치를 운용할 법적 권한조차 부여받지 못한 실정이다. 이로 인해 해당 시설들은 막대한 예산을 투입해 시스템을 구축하더라도 위급 상황 시 직접적인 대응이 불가능한 '무용지물'이 될 우려가 커, 시설 운영 주체 입장에서는 도입 자체를 기피하거나 군·경 주도 대응에 의존하여 소극적으로 대처할 수밖에 없는 구조적 모순이 존재한다.

따라서 현재까지 안티드론 시스템은 드론침입에 따른 자산 피해 파급효과가 즉각적인 발전소 및 공항 중심으로 도입되어 왔으며, 실제로 2026년까지 국제 및 국내 공항에 대한 설치가 가속화될 계획이나 타 시설은 소외되고 있는 실정이다. 이처럼 안티드론의 도입 현황 및 계획은 일부 시설에 집중되어있는 경향이 있는데, 이는 두 가지의 원인으로 분석된다.[9]

〈표 2-15〉 국가중요시설 유형별 드론 방어 시스템 현황

구분	계	전력	원자력	수력	공항	가스	석유	정부청사	기타
개소	31	9	5	4	4	3	2	2	2

자료: 국가중요시설에 대한 북한의 드론테러 위협 분석을 통한 대응방안 연구

첫째, 도입 단가가 높다. 아직 안티드론 시스템의 표준화가 이루어지지 않아 한정된 예산 내에서 국가중요시설 중에서도 파급효가 큰 시설 위주로 우선순위를 배정할 수밖에 없는 현실적 여건을 반영한다.

둘째, 법적 제약 및 운영상의 안전 문제다. 자체적인 전파방해 장비 운용은 현행 전파법상 엄격한 제약이 따르며, 물리적 타격 방식 또한 2차 피해 우려와 법적 책임 문제로 민간 시설 도입에 한계가 명확하다. 즉 도심 복합 환경에 특화된 실증적 선행 연구가 국내에 절대적으로 부족하다. 기존 도입사례와 연구는 대부분 개활지에 위치한 발전소나 공항을 대상으로 진행되어, 전파 밀집도가 높고 유동 인구가 많은 환경에 적용할 수 있는 운용 데이터와 안티드론 장비 선행 연구가 요구된다.

3. 방송시설의 드론 방호 관련 정책 및 법제 현황

가. 현 방송시설의 드론 방호 운용

현재 국가기간 방송사는 민・관・군 협력 기반의 대응 훈련으로 드론 테러 위협에 대한 보안 공백을 완화하고 있다. KBS는 정기적으로 군(수도방위사령부 예하 부대), 경찰특공대, 소방서 등 유관 기관과 합동으로 대테러 훈련을 매년 3월에 실시한다. 이밖에 KBS 경산, 소래 송신소가 드론 피폭 테러를 가정한 을지연습 기간 민・관・군 합동 훈련을 수행하였다.[40] 이는 방송시설 자체적으로 안티드론 솔루션을 도입하거나 단독 조직만으로 방어하는 데에는 한계가 있음을 인식하고, 그 대안으로 공권력의 타격 자산을 연계하는 ‘협력 모델’을 채택한 것으로 보인다. 공개된 영상 자료를 통해 현재 운용 중이라 예상되는 시나리오별 대응체계를 정리해보면 다음과 같다.[41][42]

40) 불법 드론 KBS 소래송신소 송신탑 피격, 시흥저널, 2024.08.19.

41) 경산시, ‘KBS 경산 송신소 드론 테러 대비훈련’ 준비 만전, 데일리대구경북뉴스, 2025.08.06.

42) 국가중요시설 KBS에 드론 테러..인질 구출까지 실전같은 훈련, KBS뉴스, 2024.03.06.

시나리오 : 적대 세력의 드론이 KBS 본관 상공에 침투하여 폭발물을 투하하거나, 자폭 드론이 송신탑에 충돌하여 화재가 발생하는 상황을 가정한다.

1. 대응절차: KBS 보안팀 또는 인근 군 대공감시소가 육안으로 드론을 탐지.
2. 상황전파: 관할 군부대 및 경찰청 112 상황실, 소방서에 즉시 전파.
3. 초동조치: 청사 내 인원 대피 유도, 중요 방송 장비 방호 셔터 가동.
4. 무력화 : 경찰특공대 및 군부대가 안티드론 건을 이용하여 무력화
5. 진압 : 추락한 드론의 폭발물을 처리(EOD)

현재 운용되는 '선(先) 신고 - 후(後) 출동' 방식은 현행 법·제도적 환경에서 실질적으로 운영 가능한 최선의 방식으로 생각되나, 다음과 같은 한계점이 존재한다.

첫째, 시설관리 주체의 '방호 권한 부재'로 인한 대응의 수동성이다. 현행 통합방위법 및 관련 규정상, 민간신분의 시설 보안팀은 테러 상황 발생 시 직접적인 저지나 제압을 할 수 있는 법적 권한이 부여되어 있지 않다. 이로 인해 시설 측의 역할은 단순 '탐지 및 상황전파'라는 소극적 조치에 국한될 수밖에 없으며, 이는 테러 초기 가장 중요한 골든 타임에 스스로 지키지 못하고 외부 지원만 기다려야 하는 제도적 공백을 초래할 수 있다.

둘째, 공권력 투입 절차에 따른 필연적인 '대응 시차' 발생이다. 현행 제도는 군·경 등 타격 자산이 현장에 도착한 이후에야 실질적인 무력화가 시작되는 구조다. 신고 접수부터 상황 전파, 부대 출동 및 현장 도착까지는 물리적으로 최소 10~20분이 소요되나, 실제 드론 테러는 기습 후 불과 수 분 내에 타격이 종료되는 속전속결의 양상을 띤다. 즉, 물리적인 이동 시간이 소요되는 외부 지원 중심의 방어체계는 고속 드론 위협을 방어하기에는 시차적 한계가 명확하며, 이 시간 동안 시설은 사실상 무방비 상태에 노출된다.

결국 문제의 핵심은 시설 방호 주체에게 실질적인 대응 권한이 부여되지 않고, 안티드론 시스템 운용에 대한 법적 근거와 책임 소재가 불명확하다는 점이다. 또한 현행 「전파법」은 방송시설에서 전파방해 장비 사용을 엄격히 제한해 자체 방어체계 도입에 법적 제약이 크며, 드론 격추로 인한 낙하물 피해나 인명 사고에 대해 보안 담당자를 보호할 면책 규정도 마련되어 있지 않다.

나. 방송시설의 안티드론 도입 관련 법제

1) 방송시설의 안티드론 시스템의 도입 근거

〔그림 2-35〕 국가중요시설 지정(방송시설)

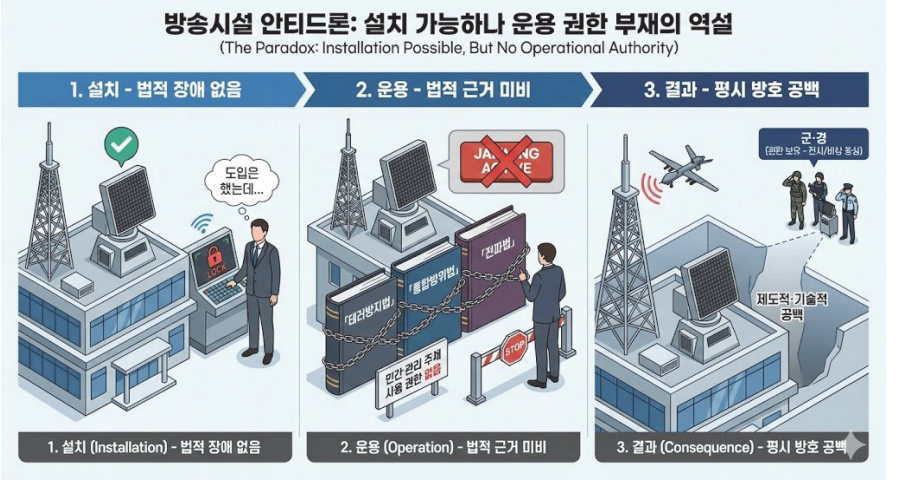
「방송법」 제85조 2에서는 정당한 사유 없이 방송을 중단하는 것을 엄격히 금지하고 있으며, 특히 KBS와 같은 재난방송 주관 방송사에게는 「방송통신발전 기본법」 제40조(재난방송 등)을 의거 했을때, 어떤 상황에서도 방송을 지속해야 할 법적 의무가 있다. 따라서 이와 같은 무중단 연속성과 안보적 중요성을 위해 방송국(특히 KBS 등)과 주요 송신소는 「통합방위법」에 따라 국가중요시설로 지정되어 관리된다.

> 방송법 제85조의 2(금지행위) ① 방송사업자 · 중계유선방송사업자 · 음악유선방송사업자 · 전광판방송사업자 · 전송망사업자(이하 “방송사업자등”이라 한다)는 사업자 간의 공정한 경쟁 또는 시청자의 이익을 저해하거나 저해할 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 “금지행위”라 한다)를 하거나 제3자로 하여금 이를 하게 하여서는 아니 된다. <개정 2015. 3. 13., 2015. 12. 22.>
>
> 1. 정당한 사유 없이 채널 · 프로그램의 제공 또는 다른 방송사업자등의 서비스 제공에 필수적인 설비에 대한 접근을 거부 · 중단 · 제한하거나 채널 편성을 변경하는 행위

현재 방송시설에서 안티드론 도입 및 운용을 위한 법적 근거는 방송시설이 국가주요시설 지정에 따른 「테러방지법」과 「통합방위법」에서 찾을 수 있다. 즉, 안티드론 시스템의 도입은 단순한 시설 보호를 넘어, 어떤 상황에서도 방송을 지속해야 하는 강력한 법적 의무를 완수하기 위한 '필수적 이행 수단'으로서 그 도입의 당위성을 갖는다.

2) 방송시설 안티드론 시스템 운용 권한 관련 법령의 한계

〔그림 2-36〕 방송시설 안티드론 운용 권한 부재의 역설

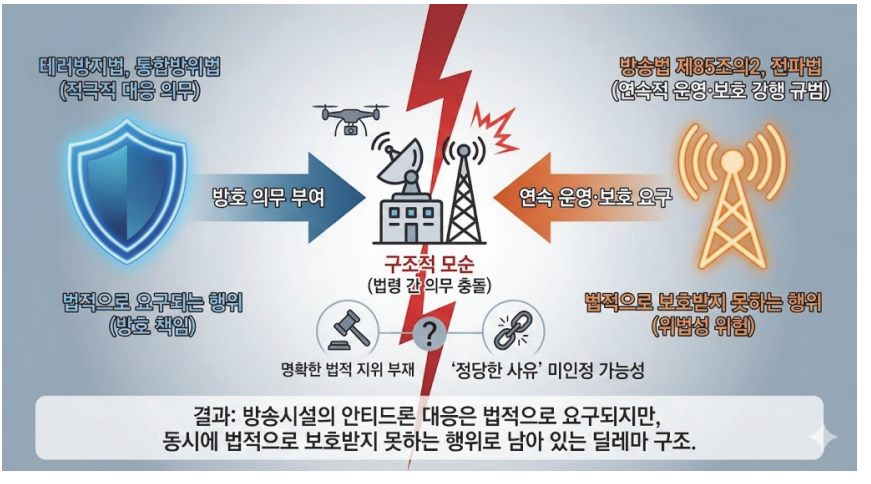


현재 방송시설의 경우 안티드론 시스템의 설치 자체를 제한하는 명시적 법적 장애는 없으나, 불법 드론에 대한 무력화·전파차단 등 적극적 대응을 수행할 수 있는 운용 권한에 대해서는 법적·제도적 근거가 마련되어 있지 않은 실정이다. 「테러방지법」, 「통합방위법」, 「전파법」 법령에 의거하면 현재 방송시설에서 안티드론 장비를 합법적으로 운용할 수 있는 권한은 오직 군·경에만 있을 뿐, 실제 시설을 방호해야 하는 방송사 등 민간 관리 주체에게는 사용 권한이 없다.

따라서 안티드론 시스템을 도입할 수 있는 법적 근거는 마련되어 있지만, 실제 직접적 운용을 할 수 있는 주체가 되지 못한다. 결과적으로 현행 제도는 전시·비상 상황 중심으로 설계되어 있어, 평시 핵심 방송 인프라 보호 관점에서는 제도적·기술적 공백이 존재한다. 이에 본 보고서 제4장에서는, 현행 법·제도의 한계를 전제로 하여 방송시설에 적용 가능한 안티드론 시스템 구축 및 운용 방안을 제시하고, 제도적·기술적 공백을 완화할 수 있는 현실적 대안을 설명한다.

3) 국가안보 관련 법령과 방송·전파 법령 간의 구조적 모순

〔그림 2-37〕 국가안보 관련 법령과 방송·전파 간의 구조적 모순



「테러방지법」과 「통합방위법」은 국가중요시설에 대해 테러 및 외부 위협으로부터 시설을 방호하기 위한 적극적 대응 의무를 부여하고 있음에도 불구하고, 「방송법」 제85조의2와 「전파법」 제 82조는 방송 및 무선설비의 연속적 운영과 보호를 강행 규범으로 요구하고 있어, 「전파법」 제 29조 '혼신 등의 방지'에서 운용 예외조항인 국가중요시설에서 안티드론 대응을 수행하는 경우 법령 간 의무 충돌이라는 구조적 모순이 발생한다. 아래는 전파법 제 82조(벌칙)에서 무선국의 무선설비가 제공하는 업무에 대해 설명하고 있다.

전파법 제82조(벌칙) ① 다음 각 호 어느 하나의 업무에 제공되는 무선국의 무선설비를 손괴(損壞)하거나 물품의 접촉, 그 밖의 방법으로 무선설비의 기능에 장해를 주어 무선통신을 방해한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <개정 2014. 6. 3.>

1. 전기통신 업무

2. 방송 업무

이하생략..

현행 「방송법」 및 「전파법」 체계는 방송시설에서 안티드론 대응을 전제로 한 전파차단 또는 무력화 조치에 대해 명확한 법적 지위를 부여하고 있지 않다. 방송시설과 그 운용 장비는 무선국 및 무선설비로 분류되므로, 방송의 중단을 제한하는 「방송법」 제85조의2와 무선설비의 정상적 운용 및 보호를 전제로 하는 「전파법」의 규정이 방호 목적의 전파차단·무력화 조치와 직접적으로 충돌할 소지를 갖는다.

또한 「방송법」 제85조의2는 방송 중단 또는 제한을 허용하는 '정당한 사유'를 명시적으로 열거하고 있지 않으며, 드론 위협 대응을 그 사유로 포함한다는 규정도 두고 있지 않다. 이로 인해 테러방지법 및 통합방위법상 방호 의무가 현행 방송법 체계에서 곧바로 '정당한 사유'로 인정된다고 법리적으로 해석하기는 어렵다. 결과적으로 방송시설의 안티드론 대응은 법적으로 요구되지만, 동시에 법적으로 보호받지 못하는 행위로 남아 있는 구조적 모순을 가지고 있다.

4. 해외 안티드론의 정책 및 법제 추진현황

가. 미국

1) FAA의 드론의 정의

2018년 이전 미국은 연방항공청이(FAA) 드론을 '항공기'로 간주했기 때문에, 드론을 향한 모든 물리, 전파적 대응이 연방법 위반으로, 이를 공격하는 행위는 마치 여객기를 격

추하거나 하이재킹하는 것과 동일한 수준의 중범죄로 취급되었다.

> Huerta v. Pirker 사건 (2014)
> 2011년, 사진작가 Raphael Pirker는 버지니아 대학교 캠퍼스 상공에서 카메라가 장착된 소형 무인항공기(드론)를 상업적 목적으로 조종했다. FAA는 Pirker가 사람, 건물, 차량 위로 낮은 고도에서 무모하고 부주의하게 비행하여 타인의 생명이나 재산을 위태롭게 했다고 주장하며 10,000달러의 민사 벌금을 부과했다. Pirker는 '모형 항공기'에 불과하며, FAA가 모형 항공기에 적용되는 공식적인 규정을 발표한 적이 없으므로 FAA의 규제 대상이 아니라고 항변했다. 행정법 판사는 Pirker의 손을 들어주며 FAA의 벌금 부과 명령을 기각했다. FAA는 이 결정에 항소했고, 2014년 NTSB 전체 위원회는 만장일치로 초기 판결을 뒤집었습니다. NTSB는 법률 및 규정의 광범위한 정의에 따라 드론을 포함한 무인 항공기가 '항공기'의 범주에 속하며 FAA의 규제 대상이라고 판결하였다.

2) 드론 탐지기의 법적 해석

2018년 이전 미국은 안티드론 시스템이 드론의 식별 정보를 얻기 위해 신호를 수신하고 해독하는 행위 자체가 그 누구든 간에 불법 감청으로 간주된다고 판단하고, 도청방지법(Wiretap Act)[43]의 위반으로 간주될 수 있다고 해석되었다[26]. 그 이유는 드론과 조종기 사이의 통신은 '공개 방송'이 아니라 '잠겨 있는 사적 대화'이기 때문이라 보기도 한다. 하지만 그 반대의 해석도 존재하였다. 항공 통신 시스템에서의 통신이 그 예인데, 항공기 조종사와 관제탑이 주고받는 교신 내용은 항공안전을 위해 공개되어야 하므로, 이를 듣는 것은 도청이 아니라고 주장하는 측면도 존재하였다. 통신비밀보호법(Wiretap Act) 제2511조[44]는 "항공 통신 시스템(Aeronautical Communications System)"의 감청을 예외적

43) 1060. Scope of 18 U.S.C. § 2512 Prohibitions, U.S. Department of Justice

44) 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic

으로 허용하고 있으며, 2018년 이전 미국은 연방항공청이(FAA) 드론을 ‘항공기’로 간주했기 때문이었다. 이는 아래에서 설명할 2018년 ‘신종위협방지법(Preventing Emerging Threats Act of 2018, S.2836)’이 제정되기 이전까지 심지어 FBI나 국토안보부(DHS) 같은 연방 수사기관조차도 안티드론(특히 무력화 및 감청) 장비를 사용하는 것이 법적으로 ‘불법’이었다.

2018년 5월 ‘신종위협방지법(Preventing Emerging Threats Act of 2018, S.2836)’에서 안티드론과 관련된 법이 제정되었다. 이 법은 국토안보부와 법무부가 별도의 사전 동의 절차 없이도 위협 드론에 대해 즉각적으로 대응할 수 있도록 규정하고 있으며, 해당 법령에 따라 이들 기관은 드론을 탐지 및 식별하는 감시 활동은 물론, 조종사에게 경고를 보내거나 제어 신호를 교란하여 조종을 방해하는 행위가 가능하도록 하였다. 더 나아가 드론의 제어권을 강제로 탈취하거나 기체를 압수할 수 있으며, 최후의 수단으로 합리적인 무력을 사용하여 드론을 파괴하거나 손상시키는 행위까지 명시적으로 허용하고 있다. 2018년 제정 당시, 이 법은 드론 기술의 변화 속도와 부작용을 고려하여 5년이 지나면 효력이 사라지는 ‘일몰 조항(Sunset Clause)’을 포함하였었다. 따라서 2024년 제정된 기존 법률의 효력은 만료되었으며, 2024년 발의되었던 무인항공기 대응 권한 보안, 안전 및 재승인 법안 (HR8610)이 통과되었었다[27].

2023년 6월 무장화된 드론(UAS)은 대규모 인파가 모이는 시설과 공공안전에 심각한 위협이 되고 있으나, 현재 미국 법체계는 연방 기관(DHS 등) 중심으로만 탐지 및 대응 권한을 부여하고 있어 주・지방 경찰 및 민간 시설 보안 주체는 실질적 대응이 불가능한 상황으로 주・지방 경찰 및 대중시설 보안 주체까지 탐지・무력화 권한을 확대를 주장하였다.[45]

communications prohibited, Legal Information Institute

45) Protecting Mass Gathering Venues Against Drone Threats: How SIA and the Industry Are Leading the Way, Security Industry Association (SIA), 2023.06.05.

2025년 12월, 미국 대통령은 2026 회계연도 국방수권법(FY2026 NDAA)을 최종 서명 및 공포하였다.[46] 이번 법안에는 안티드론 대응 역량을 대폭 강화하는 내용이 포함되어 있으며, 특히 제86장에 수록된 ‘SAFER SKIES 법안’은 국토안보부(DHS)와 법무부(DOJ)를 포함하여 특정 주(State) 및 지방 기관까지 무인항공기 대응 활동 범위를 확장하는 데 중점을 두고 있다[28]. 주목할 점은, 이 권한은 연방 기관을 넘어 주(State) 경찰이나 지방(Local) 경찰 등 비연방 공공 기관(SLTT)[47]에 위임될 수 있으며, 즉, 이전에는 지방에서 테러 위협이 현지 경찰은 드론을 무력화할 수 없었으나, 해당법으로 이것이 가능하도록 보장하는 것이다. 따라서 이 법안이 통과되면, 대규모 공공 행사 및 장소, 공공장소, 중요 기반시설, 교도소 및 구치소와 같은 교정 시설을 포함한 여러 특정 상황이 고려될 것으로 보인다. 아래는 자세한 규정이다.

NDAA 제8602조는 ‘공공 안전 보호를 위한 드론 대응책’을 규정하였다. 이는 기존 연방 법률을 개정하여 국토안보부(DHS)와 법무부(DOJ)가 국가중요시설이나 대규모 행사 등 공공안전에 심각한 위협이 되는 무인항공기를 탐지하고 추적하며, 나아가 위협을 완화(Mitigation)할 수 있는 권한을 확대 부여하였다. 이를 통해 연방 기관은 더욱 폭넓은 장소와 상황에서 능동적인 방어 조치를 취할 수 있게 되었다.

NDAA는 에너지부(DOE) 산하 원자력시설의 방호 권한을 명시하였다. 제3111조에 따르면, 에너지부는 원자력시설을 위협하는 무인항공기에 대해 즉각적인 조치를 취할 수 있는 강력한 법적 권한을 갖게 되었다. 에너지부는 위협 드론을 탐지, 식별, 모니터링 및 추적할 수 있을 뿐만 아니라(Section 3111(b)(1)), 드론 제어에 사용되는 통신 신호를 포착하여 가로채는 감청 행위까지 허용받았다(Section 3111(b)(2)). 나아가 운영자에게 경고를 보내거나(Section 3111(b)(3)), 필요시 합리적인 무력을 사용하여 드론을 방해, 압수, 몰수하거나 물리적으로 파괴 및 무력화할 수 있는 권한까지 확보하였다(Section 3111(b)(4)).

---

46) President Trump Signs FY2026 National Defense Authorization Act into Law, Office of Rep. Rick W. Allen (Press Release), 2025.12.18.

47) SLTI(State:주 정부, Local:지방 정부, Tribal:원주민 자치정부, Territorial:미국 해외 영토 정부)

2025년 12월 새로운 국방수권법(NDAA)이 통과되면서, 기존에 교통인프라위원회(T&I)에서 추진하던 별도의 안티드론 법안(HR 5061)이 무산될 상황이 발생하였다.[48] HR 5061의 주요 내용은 안티드론 권한을 단순히 확대하는 것이 아니라 전면적인 권한 부여 이전에, 검증된 일부 법집행기관을 대상으로 'Counter-UAS Mitigation Law Enforcement Pilot Program'을 신설하여 점차적으로 합리적으로 확대하는 것이 목표였다.[49] 이 법안의 가장 큰 특징은 미국 FAA의 역할을 핵심적으로 유지하여, FAA가 주도하에 국토안보부 및 법무부와 협력하여 안티드론 기술의 안전성을 검증해 나가면서 시범적 운영하는 것을 목표로 하였었다. 반면, 통과된 NDAA는 신속하게 대응 태세를 갖추는 법안이라고 볼 수 있다.

나. 유럽

2018년 12월 발생했던, 영국 개트윅(Gatwick) 공항 드론 사태 때 3일 공항이 마비되는 일 발생 이후 안티드론 시스템 부재의 심각성이 대두되었다.

2019년 10월 유럽항공안정청(EASA)은 'Counter Drones (C-UAS) action plan'을 통해 5대 C-UAS 실행 계획을 발표하였다[29].

> 유럽항공안정청 C-UAS 5 Action Plan:
> 1. 대중 교육: 공항 주변 드론 오용 방지 및 감소
> 2. 공항 준비 태세: 무단 드론 사용으로 인한 위험 완화 준비
> 3. 위험 평가 지원: 드론이 유인 항공기에 미치는 안전 위험을 과학적 평가
> 4. 안티드론 조치: 안티드론 도입의 가이드라인
> 5. 보고체계 지원 : 적절한 사고 발생 보고체계 지원

유럽의 경우 유럽연합(EU)이라는 태생적, 법적 한계로 인해 탐지와 무력화가 분리된

48) C-UAS provisions in US NDAA 2026 throw pending bipartisan legislation into question, Unmanned Airspace, 2025.12.15.

49) T&I Approves Bipartisan Bill to Reauthorize and Reform Counter-UAS Authorities, U.S. House Committee on Transportation & Infrastructure, 2025.09.03.

대응구조가 확립되었다. 즉 EASA(유럽항공안전청)는 EU 기구이지만, 경찰과 군대는 프랑스, 독일 등 개별 국가의 소유로, 규제(Regulation)로 인해 '항공 안전(Safety)'에 대해 명령할 수 있지만, 드론에 대한 무력화/교란의 책임은 각 국가 법 집행 규정에 속한다고 명시하였다. 즉 드론의 탐지 및 식별 시스템 구축은 공항 운영자의 책임으로 두되, 실제로 드론을 격추하거나 재밍하는 무력 사용 권한은 각 회원국의 경찰 및 사법 당국의 고유 권한으로 명확히 분리한 것이다.

2020년 12월 예전에는 드론이 발신하는 RF 신호(MAC 주소, 시리얼 넘버) 역시 데이터 컨트롤러(조종자)를 식별할 수 있는 고유한 값이므로 개인정보(Personal Data)에 해당한다.[50] 따라서, 단순 모니터링은 가능하지만 저장하게 되면 GDPR 제6조(처리 적법성) 위반 문제가 있다는 의견이 나왔다.[51] 따라서, 'Regulation (EU/UK) 2019/945 및 Regulation (EU) 2019/947'을 기반으로 합법적인 안티드론 탐지 근거 수단을 마련하였고[30][31], 드론 제조사에게 'Remote ID(원격 식별 장치)'를 내장해서 항상 자신의 위치를 송출하도록 강제했다.

〈표 2-16〉 무게에 따른 등급과 Remote ID 의무

등급	무게	Remote ID 의무
C0	250g 미만	면제
C1	900g 미만	의무
C2	4kg 미만	의무
C3 ~ C6	25kg 미만	의무
레거시	-	의무

자료: FAA의 원격 식별 정책, EASA REMOTE ID REQUIREMENTS 등을 참고하여 재구성

1) 영국

2021년 10월 영국은 2021년 제정된 「항공교통관리 및 무인항공기법(ATM & UA Act

50) Art. 6 GDPR – Lawfulness of processing, General Data Protection Regulation (GDPR)

51) GDPR Compliance for Drone Operators: Handling Captured Data Responsibly, GDPR Advisor

2021)」을 통해 경찰의 드론 대응 권한을 완성하였다[52]. 동 법안의 Schedule 9를 통해 기존 「무선전신법 2006(Wireless Telegraphy Act 2006)」을 개정하였다. 이를 통해 내무부 장관이 지정하고 OFCOM(통신청)이 기술적으로 승인한 안티드론 장비(전파 차단 장치)를 사용하는 경우, 이를 전파법 위반의 예외로 인정하는 '합법적 면책(Legal Exemption)' 조항을 신설하였다.[53]

국내와 유사하게, 영국의 기존 무선전신법은 '고의적 방해(Deliberate Interference)'를 금지하고 있었으나, 안티드론 방어(Counter-UAS)를 위한 예외조항을 신설하여, 국무장관(Secretary of State)이 승인한 공공안전 목적의 드론 무력화 장비 사용은 전파법 위반으로 보지 않도록 개정하였다. 여기서 사용될 수 있는 장비는 OFCOM(통신청)과 협의하여 해당 장비가 민간 항공이나 병원 통신 등 다른 중요 주파수에 간섭을 일으키지 않는지 기술적으로 검증된 장비를 일컫는다.

2) 기타 유럽국가

2023년 8월 프랑스는 2024 파리 올림픽을 계기로, 「국내보안법」, '무인 항공기로부터 발생하는 위협에 대한 보호 (제L213-2조)'을 신설하였다. 총리가 지정한 국가중요시설을 포함한 지역 상공을 해당 항공기가 비행하는 것을 방지하기 위해, 총리의 명령으로 지정된 장치를 사용하여 무인항공기를 무력화하거나 작동 불능 상태로 만들 수 있다고 명시하였다. 이로써 안티드론 대응 권한을 법률에 매우 구체적이고 명시적으로 규정하였다.[54]

52) Air Traffic Management and Unmanned Aircraft Act 2021, UK Legislation (legislation.gov.uk), 2021.12.

53) Wireless Telegraphy Act 2006, UK Legislation (legislation.gov.uk), 2006

54) Code de la sécurité intérieure, Légifrance (République française), 2025.12.13.

제3장 위험 분석 기법 기반 연구 방법론 및 적용

제1절 위험 분석 기법 개요

본 절에서 수행하는 위험 분석은 방송시설 보호를 목적으로, 자산·위협·위험의 개념을 구분하여 체계적으로 평가하는 과정이다. 이를 위해 다음과 같은 기본 개념을 정의한다.

먼저 자산(Asset)이란 보호가 필요한 대상으로서, 방송송출의 연속성과 품질 유지, 인명 안전, 공공 서비스 제공에 필수적인 시설·설비·주파수 자원 등을 의미한다. 본 연구에서는 주조정실, 송·중계소 설비와 같은 유형 자산과, 방송 주파수 및 중계 링크와 같은 무형 자산을 모두 자산 범주에 포함한다.

위협(Threat)이란 자산에 피해를 유발할 수 있는 잠재적 원인으로, 본 연구에서는 불법·적대적 드론 행위뿐 아니라 안티드론 시스템 운용 과정에서 발생할 수 있는 전파 간섭, 고출력 전파 방사, 요격 잔해 낙하 등 부수적 요인까지 포함한다. 즉, 위협은 자산에 영향을 줄 수 있는 행위 또는 사건 자체를 의미한다.

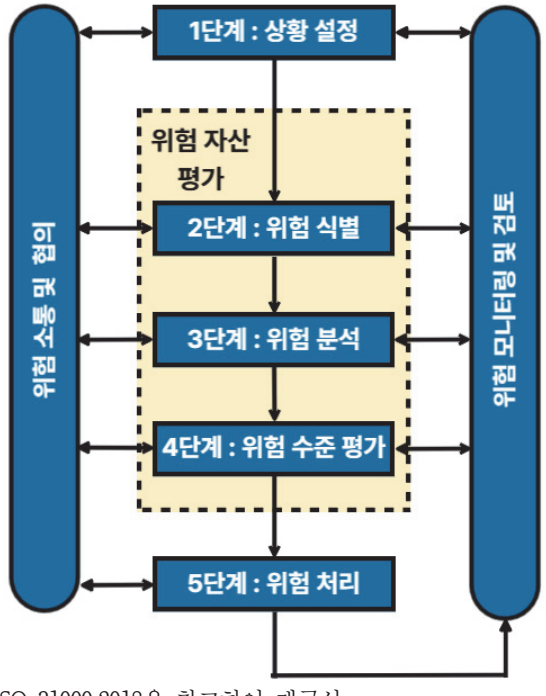
위험(Risk)은 특정 위협이 자산에 작용할 경우 발생할 수 있는 피해의 가능성과 그 영향의 결합으로 정의된다. 다시 말해, 위험은 단순히 위협이 존재하는 상태가 아니라, 해당 위협이 실제로 발생할 가능성과 발생 시 자산에 미치는 영향의 크기를 함께 고려한 결과이다.

마지막으로 위험을 분석한다는 것은 식별된 자산과 위협을 연결하여 위험 시나리오를 구성하고, 각 위험을 분석·비교함으로써 발생 가능성과 피해 영향 수준을 종합적으로 판단하는 것을 의미한다. 이를 통해 어떤 자산이 우선적으로 보호되어야 하는지, 어떠한 위협에 대해 대응이 필요한지, 그리고 기술적·운영적 대응 수준을 어디까지 설정해야 하는지를 체계적으로 도출할 수 있다.

본 연구에서는 방송시설의 보호 자산을 대상으로, 불법·적대적 드론으로 인한 직접적 위협과 안티 드론 시스템 운용 과정에서 발생할 수 있는 전파 교란, 통신 간섭, 장비 손상 등 연계 위험을 통합적으로 고려하여 위험 평가를 수행한다. 방송시설의 체계는 전파·제어·센서·물리적 환경이 결합된 사이버-물리 시스템(Cyber-Physical System, CPS)의 특

성을 가지므로, 본 절에서는 범용적으로 사용되는 ISO 31000의 위험관리 체계를 기본 틀로 삼고, 국내표준인 KS X ISO/IEC 27005가 제시하는 세부 절차에 따라 분석을 수행한다.

〔그림 3-1〕 ISO 31000 (위험관리 표준) 기반 위험 평가 과정



자료: ISO 31000:2018을 참고하여 재구성

위험 분석 기법은 ISO 31000(위험관리 표준)에 근거한다. 이에 따라 ① 상황 설정 (Establish Context), ② 위험 식별 (Risk Identification), ③ 위험 분석 (Risk Analysis), ④ 위험 평가 (Risk Evaluation), ⑤ 위험 대응 (Risk Treatment)의 순차적 절차를 따른다.

상황 설정 단계에서는 위험 평가의 목적과 범위를 규정하며, 위험 식별 단계에서는 보호 자산과 관련 위협·취약점을 도출한다. 위험 분석 단계에서는 발생 가능성과 영향도를 산정하여 위험 수준을 계산하고, 위험 평가 단계에서는 산출된 위험 수준을 기준에 따라 판단한다. 마지막으로 위험 대응 단계에서는 위험 저감 또는 수용 등 적절한 대책을 마련한다.

제 2 절 방송시설 상황 설정(Establish Context) 단계

1. 방송시설 상황 설정 단계 개요

본 절은 ISO 31000에서 제시하는 상황 설정 절차를 설명하기 위한 것으로, 위험관리 활동이 수행될 목적, 범위, 기준을 명확히 정의하여 이후 평가까지의 과정을 조직 환경에 적합하게 적용하는 것을 목표로 한다. 상황 설정 단계는 다음의 세 가지 요소로 구성된다.

○ 범위 설정: 위험관리 활동이 적용될 대상과 한계를 규정하는 절차
○ 내외부 환경의 이해: 위험이 발생하고 영향을 미치는 배경 조건을 분석하는 절차
○ 위험 기준 설정: 위험의 중요도를 판단하기 위한 기준과 판단 체계를 마련하는 절차

2. 평가 범위(Scope) 설정

가. 평가 범위 설정 방법

평가 범위 설정은 위험관리 활동의 적용 대상과 경계를 명확히 규정하는 단계이다. ISO 31000은 위험관리 프로세스가 전략적, 운영적, 프로그램 단위, 프로젝트 단위 등 다양한 수준에서 적용될 수 있음을 전제로 하기 때문에, 평가 대상의 수준과 목적을 명확히 하는 것이 중요하다. 범위 설정 시 고려해야 할 항목은 <표 3−1>과 같다.

〈표 3−1〉 평가 범위 설정에 요구되는 주요 항목

구 분	주요 내용	적용 범위
목표 사항	위험 관리 과정이 지원해야 할 조직의 목표는 무엇인가?	Y
기대 결과	위험 평가 수행을 통해 도출하고자 하는 산출물은 무엇인가?	Y
시공간적 범위	평가가 적용될 기간과 장소를 어떻게 규정할 것인가?	Y
포함・제외 조건	포함・제외될 자산・시스템은 무엇인가?	Y
분석 방법	어떤 위험 평가 도구 및 분석 방법을 사용할 것인가?	Y
필요 자원 분석	평가 수행에 필요한 인적・기술적 요구사항은 무엇인가?	N
연계성	다른 내・외부 조직 활동과 어떤 연계성이 있는가?	Y

자료: ISO 31000:2018을 참고하여 본 연구에 맞게 재구성

본 연구는 외부 전문기관 수행 연구로서 방송시설의 내부 운영 정보에는 접근할 수 없으므로, 해당 항목은 ‘적용 불가(N)’로 분류하였다. 반면 연구 목적, 자산군, 위험 평가 방법론 등 외부 기관 관점에서 정의 가능한 요소는 ‘적용(Y)’으로 설정하여 정책연구에 적합한 평가 범위를 구성하였다.

나. 방송시설 대상 평가 범위

본 연구의 위험관리 범위는 방송송출에 직접적으로 영향을 미치는 방송시설·전송망·주파수 운용체계 전체를 대상으로 설정한다. 방송시설은 국가 중요 통신 인프라로서, 송신 장비, 중계 설비, 전파관리 체계, 제어·모니터링 시스템 등 다수의 핵심 자산으로 구성되어 있으므로 평가 범위를 명확히 구분하는 것이 필수적이다. 이에 따라 범위 설정 항목은 다음과 같이 방송시설 환경을 기준으로 구체화하였다.

1) 목표 사항

본 연구는 방송시설의 공공 인프라로서의 특수성과 변화하는 드론 위협 환경을 고려하여, 방송시설 보호에 적합한 위험 분석 체계와 안티드론 운용 기준 마련을 목적으로 한다.

이를 위해 본 연구는 다음과 같은 사항을 중점적으로 도출하고자 한다.

○ 방송시설 특수성을 반영한 드론 위협 및 무력화 기술의 위협을 체계적 식별·분석

- 방송송출 연속성, 전파 혼신 민감도, 설비 의존성 등 방송시설 고유 특성을 고려한 위험모델 구축

○ 위험 평가 결과를 기반으로 방송시설에 적합한 안티드론 구축 방안을 도출

- 기술별 위험 수준 산출
- 산출 결과와 제도적 측면을 근거로 안티 드론 구축 방안 마련

○ 방송시설 보호체계 강화를 위한 운영·배치·기관연계 가이드라인을 제시

- [방송사-군·경·대테러 센터] 연동 체계 제시
- 정책·제도 개선이 가능한 수준의 기준 제시

2) 기대 결과

본 연구의 위험 평가는 상황 설정, 위험 식별, 위험 분석, 위험 평가, 위험 대응의 단계로 구성되며, 각 단계별로 다음과 같은 결과와 산출물을 도출한다.

○ 상황 설정 단계에서의 기대 결과 및 산출물

- 위험 평가 범위(Scope)
- 조직의 내·외부 환경(Context)
- 위험 기준(Risk Criteria)

○ 위험 식별 단계에서의 기대 결과 및 산출물

- 방송시설 핵심자산(Asset) 목록 및 구조
- 드론과 안티드론 기술이 결합된 위협(Threat) 시나리오 목록

○ 위험 분석 단계에서의 기대 결과 및 산출물

- 위협 시나리오에 따른 영향도(Impact)
- 위험 요인의 발생 가능성(Likelihood)
- 영향도와 발생 가능성을 결합한 위험 수준 산정표(Risk Level Matrix)

○ 위험 평가 단계에서의 기대 결과 및 산출물

- 위험 허용 기준(Risk Acceptable Criteria)
- 방어체계 구축에 따른 위험 모델 결과

○ 위험 대응 단계에서의 기대 결과 및 산출물

- 위험 수준에 따른 대응 전략(회피·저감·수용) 정의
- 대응 우선순위 및 방어체계 유형에 따른 위험 수준 이동

3) 시공간적 범위

본 연구는 방송시설을 둘러싼 드론 위협이 특정 시점이나 단일 공간에 한정되지 않고, 운영 조건과 전파 환경의 변화에 따라 달라질 수 있다는 점을 고려하여 시공간적 범위를

설정하였다. 이에 따라 위험 평가는 시간적 범위와 공간적 범위를 구분하여 수행한다.

○ 시간적 범위

현행 방송운영 환경을 기준으로 하되, 향후 변화 요인까지 포함하여 시간 범위를 설정

- 2025년 현재 방송시설 환경 및 전파관리 조건
- 평시·위기·전시 등 운영 조건 변화 시나리오
- 향후 3~5년 내 기술·규제 변화(드론 기술 고도화, 전파정책 변화 등) 고려

○ 공간적 범위

- 연주소, 송신소, 중계소 등 방송송출이 이루어지는 핵심 운영 지역
- 송출 제어·전파 모니터링·전송 운영이 이루어지는 기능구역
- 전파 간섭 가능성이 존재하는 인근 외부 공간

이와 같이 설정된 시공간적 범위는 위험 평가가 현재 운영 환경에 국한되지 않고, 다양한 운영 조건과 시설 배치 상황을 포괄할 수 있도록 하기 위한 것이다. 이를 통해 방송시설 전반에 대한 드론 위협과 대응 필요성을 보다 현실적으로 분석하고자 한다.

4) 포함 및 제외 조건

본 연구의 위험 평가는 방송시설 보호라는 목적에 부합하도록, 방송송출과 전파 운용에 직접적인 영향을 미치는 핵심 자산을 중심으로 범위를 설정한다. 이에 따라 위험 평가의 실효성을 높이기 위해 평가에 포함되는 자산과 제외되는 자산을 명확히 구분하였다.

○ 포함 범위

- 송·수신 RF 시스템
- 송신 안테나 및 전파 방사 시스템
- 수신 안테나 및 전파 수신 시스템
- 송·수신 인프라 및 환경
- STL·TTL 등 방송전송망 및 관련 장비
- 전파 운용 채널

○ 제외 범위

- 콘텐츠 제작 공간(스튜디오, 편집실, 자막·CG 제작 관련 설비 등)
- 사무공간 및 일반 행정시설(회의실, 인사·회계 시스템 등)
- 일반 IT 시스템(ERP, 그룹웨어, 내부 업무용 파일서버 등)
- 대외 서비스용 설비(홈페이지 서버, 외부 홍보시스템 등)
- 방문객 구역 및 일반 출입구역 등 비운영 공간

이와 같은 포함·제외 기준은 위험 평가의 범위를 방송송출과 전파 운용에 직접적인 영향을 미치는 영역으로 한정함으로써, 드론 위협이 실제 방송서비스와 설비 안정성에 미치는 영향을 보다 집중적으로 분석하기 위한 것이다. 이를 통해 평가 범위의 과도한 확장을 방지하고, 위험 분석 결과의 실효성과 활용성을 높이고자 한다.

5) 분석 방법

본 연구는 방송시설 보호를 위한 위험 분석을 수행하기 위해, ISO 31000 및 KS X ISO/IEC 27005에서 제시하는 위험관리 절차를 기반으로 위험 평가체계를 적용한다. 해당 체계는 방송시설의 자산 구조와 전파 운용 특성을 반영하여, 드론 위협과 안티드론 기술 운용에 따른 위험을 체계적으로 도출·분석하는 데 목적이 있다.

○ ISO 31000 및 KS X ISO/IEC 27005 기반 위험 평가체계 적용

- [상황 설정 → 위험 식별 → 위험 분석 → 위험 평가 → 위험 대응]의 절차에 따라 구조적으로 수행
- 방송시설의 자산 구조와 전파 운용 특성을 반영하여 평가 기준·스케일·절차를 표준화
- 국제표준(ISO 31000)과 국가표준(KS X ISO/IEC 27005)을 고려해 드론 위협 및 무력화 기술의 위험요인을 체계적으로 도출·분석

본 연구의 위험 평가는 정성적 평가를 중심으로 수행되며, 방송시설의 공공성·운영 특성·전파 민감도를 종합적으로 고려하여 위험 수준을 도출한다.

○ 정성적 평가 기반 위험 수준 도출 방식 도출

- 정성적 평가를 방송시설이 수행하는 공공적 기능과 송출 연속성에 미치는 영향을 중심으로 적용한다.
- 드론 위협 또는 안티드론 시스템 운용으로 인해 발생할 수 있는 방송 중단 가능성, 시설 및 인명 피해, 전파 혼신에 따른 서비스 품질 저하 가능성 등을 주요 판단 요소로 고려한다.
- 각 위협 시나리오는 사전에 정의한 위험 수준 기준에 따라 평가되며, 이를 통해 운용 유형별 상대적 위험 수준을 비교·분석한다.

정량적 평가 방식은 본 연구에서 고려하지 않는다. 드론의 침입, 폭발, 위협물 투하 등의 사건이 방송시설에 영향을 끼치는 사례가 전무하여 이를 수치화하기 어렵다.

6) 연계성

본 연구는 방송시설을 대상으로 한 드론 위협 분석과 위험 평가에 그치지 않고, 연구 결과가 실제 정책·제도, 대응체계, 현장 운영으로 연계·확산될 수 있도록 하는 데 목적이 있다. 이에 따라 정책·제도적 활용, 유관 기관 간 협력, 방송시설 내부 인식 제고 측면에서의 기대 효과를 다음과 같이 정리한다.

○ 정책·제도 연계 강화

- 연구 결과는 방송시설 보호 지침, 드론 대응 매뉴얼, 국가중요통신기반 보호 정책 등 제도 개선에 활용
- 주파수 관리 제도, 전파 혼신 대응 기준 등 관련 규제체계와 연계
- 정책결정기관(방송통신위원회 등)에 제공할 근거자료로 기능

○ 유관 기관(군·경·대테러센터) 연계체계 구축

- 군·경·대테러센터 등 드론 대응 주체들과의 탐지·신고·대응 프로세스를 연계
- 방송시설에서 발생하는 드론 위협에 대한 실시간 정보 공유 및 대응 마련
- 안티드론 운용체계를 군, 경, 재난통신망과 연계할 수 있는 구조 제시

○ 방송시설 내부의 위험 인식 제고

- 방송국 송출·기술 인력이 드론 위협과 전파 혼신 가능성에 대한 인식 수준을 높이는 기반 마련
- 시설 운영자에게 드론 기반 위협의 심각성과 대응 필요성을 전달하는 교육·인식 제고 자료로 활용
- 연구 결과를 바탕으로 방송시설 내부 보안·운영 프로세스 개선 필요성 환기

3. 내·외부 환경(Context)의 이해

가. 내·외부 환경의 이해 방법

내·외부 환경의 이해는 위험관리 활동이 수행될 배경을 설정하고, 위험의 원인과 영향을 해석하기 위한 기본 전제이다. 본 단계에서는 위험관리 프로세스가 적용되는 환경 조건을 구조적으로 파악하기 위한 검토 항목을 제시하며, 내부 환경은 외부 연구의 특성을 고려하여 기관 제공 자료 및 공개 가능한 정보 범위 내에서 검토한다. 본 연구의 내·외부 환경의 이해는 <표 3-2>의 항목을 고려하여 수행된다.

〈표 3-2〉 내·외부 환경 이해를 위한 주요 항목

구분	항목	주요 내용	적용 범위
내부 환경	운영 구조	조직 내 역할·책임 체계는 어떻게 구성되어 있는가?	N
	자원 체계	인력·기술·설비 등 가용 자원의 수준은 어떠한가?	N
	정책 체계	운영에 적용되는 정책·절차·규정은 무엇인가?	N
	의사결정	의사결정 과정과 권한 배분은 어떻게 이루어지는가?	N
	운영 조건	조직 내부 운영환경에서 고려해야 할 제약·특성은 무엇인가?	N
외부 환경	법·제도	적용되는 법령·규제는 무엇인가?	Y
	기술 동향	기술 변화가 위험요인·대응역량에 어떤 영향을 미치는가?	Y
	사회·환경 조건	사회·경제·지리적 환경은 위험요인에 어떤 영향을 주는가?	Y
	이해관계자	외부 기관·협력자 등 관계는 어떻게 구성되어 있는가?	Y
	외부 요인	조직 외부에서 작용하는 영향 요인·제약 요소는 무엇인가?	N

자료: ISO 31000:2018을 참고하여 본 연구에 맞게 재구성

본 연구는 외부 전문기관에 의해 수행되는 정책연구의 특성상, 기관 내부 운영 구조·자원·의사결정 체계 등 비공개 정보에 대한 접근이 제한되므로 내부 환경 항목은 검토 대상(N)에서 제외하고, 기관이 제공하는 자료 및 공개 가능한 정보 범위 내에서만 참고하였다. 외부 환경 항목 중에서도 내부 운영 특성에 대한 세부 이해가 필요한 '외부 요인'은 직접 확인이 곤란하여 검토 대상(N)에서 제외하였다. 반면, 법·제도, 기술 동향, 사회·환경 조건, 이해관계자 등 공개적으로 확인 가능한 외부 환경 항목(Y)은 위험 식별과 평가의 근거로 폭넓게 검토하였다.

나. 방송시설 대상 내부 환경의 이해

내부 환경과 관련된 항목은 본 연구에서 직접적인 분석 대상으로 포함되지 않는다.

다. 방송시설 대상 외부 환경의 이해

1) 법과 제도

방송시설의 드론 대응은 기술적 가능성뿐 아니라 현행 법·제도 내 적용 가능성을 함께 고려해야 하며, 특히 전파 이용 및 항공 안전 관련 법령은 안티드론 기술의 적용 범위와 방식에 직접적인 제약 요인으로 작용한다. 이에 본 연구에서는 방송시설 보호와 관련된 주요 법·제도를 중심으로 적용 가능성과 한계를 검토하였다.

○ 전파법 제 29조(혼신 등의 방지)의 적용 범위와 방송시설 적용 가능성

- 전파법 제29조는 전파 혼신 방지를 기본 원칙으로 하고, 공공안전 목적에 한해 전파차단장치(Jammer) 사용을 예외적으로 허용함
- 허용 대상은 대통령 경호, 군사활동, 대테러활동, 공항 안전, 원자력시설 방호 등 특정 고위험 분야로 한정됨
- 방송시설은 전파차단장치 사용 허용 범위에 포함되지 않음
- 방송시설은 현행 법령상 전파 간섭·차단 기반 기술(Jamming)을 직접 운용할 수 없음

○ 안티 드론 대응에 대한 면책 조항의 부재

- 2024년 「전파법」 개정으로 전파차단장치 운용에 대한 손실보상 기준은 마련되었으나, 형사책임은 여전히 개별 사안별 판단 구조에 머물러 있음
- 전파차단 기반 소프트킬은 제도적 인정이 이루어진 반면, 하드킬 및 복합 대응 수단에 대한 면책 범위는 명확히 규정되지 않음
- 이로 인해 안티드론 대응 전반에 대해 포괄적인 면책 체계는 부재하며, 대응 방식에 따라 법적 불확실성이 지속됨

검토 결과, 방송시설의 안티드론 대응은 기술적 구현 가능성과 달리 현행 전파법 등 법·제도 체계 하에서 적용 범위가 구조적으로 제한됨을 확인하였다. 전파차단장치는 공공안전 목적에 한해 예외적으로 허용되나, 방송시설은 적용 대상에 포함되지 않아 전파 간섭·차단 방식의 직접적 대응은 법적 제약을 받는다.

2) 기술 동향

최근 드론 기술 환경은 ‘드론의 낮은 비용과 손쉬운 접근성’, ‘비정형·개조형 드론의 증가’, ‘드론 운용자 신원 확인의 어려움’ 등으로 특징되며, 이러한 변화는 방송시설을 대상으로 한 드론 위협을 특정 상황에 국한되지 않은 상시적 위험 요소로 변화시키고 있다. 이에 따라 방송시설 상공에 대한 고의적·우발적 접근 가능성이 구조적으로 확대되고 있으며, 드론 위협은 일시적 사건이 아닌 지속적으로 관리해야 할 요인으로 인식되고 있다. 이로 인해 발생되는 위험 요인과 요구되는 대응 역량은 다음과 같다.

○ 드론의 낮은 비용과 손쉬운 접근성

[발생되는 위험 요인]

- 상업용 드론의 가격 하락으로 개인이 부담 없이 구매할 수 있는 환경이 형성
- 자동비행·안정화 기능 확대로 초보자도 단시간 내 조작 가능
- 저가 부품 기반의 개조 드론 제작이 용이, 위협 행위의 경제적 장벽이 낮아짐
- 전시 상황이 아니더라도 다양한 유형의 드론 접근 가능성 증가
- 방송시설 상공에 대한 고의 침입 시도가 상시 발생할 수 있는 환경

[요구되는 대응 역량]

- 드론 위협이 24/365 형태로 발생할 수 있어 상시 대응체계 구축 필요
- 다양한 스펙의 기체까지 탐지·식별할 수 있는 기술 역량 요구
- 단기간 접근·저고도 침입 등 기동 특성에 대응을 위한 조기경보 체계 필요
- 반복적·소모성 위협에 대비하여 연속적 감시·관제 기능 확보 필요

○ 비정형 드론의 증가

[발생되는 위험 요인]

- 표준 규격을 따르지 않는 비허가 주파수 기반 드론 제작이 가능하여 기존 감지·식별 체계의 대응 범위를 벗어날 가능성 증가
- 초소형·초경량 드론의 경우 레이다 기반 탐지 체계로 인지 어려움
- 비행 특성 및 전파 패턴이 다양하여 기존 상용 드론 분석 모델의 적용 제한됨

[요구되는 대응 역량]

- 주파수, 형상 등 비정형 드론의 범위 확장을 고려한 탐지 아키텍처 구축 필요

○ 신원확인의 어려움

[발생되는 위험 요인]

- 비행금지구역·지오펜싱 기능이 적용된 기체라도 개조 또는 오픈소스 펌웨어 변경을 통해 우회 가능
- 기체 등록 및 전자식별 기능이 적용되지 않은 드론의 광범위한 사용으로 운용자 추적이 어려움
- 공격 의도가 있는 경우 조종자 신원을 은폐한 상태로 침입·정찰·탐색 수행이 가능하여 실시간 대응에 제한 발생

[요구되는 대응 역량]

- 신원 관련 정보를 최대한 확보하기 위한 다중 센서 기반 탐지 기능 확보 필요
- 익명성 기반 위협을 고려한 상시 관제 및 기관 간 정보 공유 체계 강화 필요

3) 사회 환경 조건

방송시설은 공공적 기능과 국가 기반시설로서의 성격을 동시에 가지는 특수한 공간으로, 드론 위협이 단순한 물리적 침해를 넘어 사회적 혼란, 경제적 손실, 지리적 제약에 따른 위험 확대로 이어질 가능성이 크다. 특히 방송송출의 연속성과 전파 운용의 안정성이 직접적으로 사회 전반에 영향을 미친다는 점에서, 드론 위협에 따른 위험 요인은 다차원적으로 검토될 필요가 있다.

○ 사회적 위험 요인

- 방송국은 공영적 기능을 수행하므로 드론 위협 발생 시 사회적 파급력이 큼
- 방송 연속성 유지가 필수적, 단기 장애도 사회 혼란으로 이어질 가능성 높음
- 사회·언론의 주목도가 높은 시설로 의도적 과시비행·시위성 접근의 표적이 되기 쉬움

○ 경제적 위험 요인

- 방송송출·중계·전파 설비 등은 고가 장비로 구성되어 있어 소형 드론 충돌만으로도 막대한 경제적 피해가 발생할 수 있음
- 핵심 장비의 국산화율이 낮아 손상 시 복구 비용과 조달 기간이 크게 증가함
- 방송시설은 국가중요시설로서 장애 발생 시 직·간접 경제적 손실이 대규모로 확대될 가능성이 높음

○ 지리적 위험 요인

- 주요 송출시설은 고지대·군 관리지역 등에 위치해 접근 경로나 감시 사각지대가 발생하기 쉬움
- 방송국은 인구 밀집지역에 위치하는 경우가 많아 드론 충돌·추락 시 2차 피해 규모가 커질 수 있음
- 도시 구조물·지형 영향으로 탐지·추적 성능이 제한되어 위협 식별·대응 난도가 증가함

이와 같은 사회·경제·지리적 특성은 방송시설이 일반 시설에 비해 드론 위협에 더욱

취약한 구조적 조건을 가지고 있음을 보여준다.

4) 이해 관계자

방송시설을 대상으로 한 드론 위협 대응은 단일 기관의 역할만으로 수행되기 어렵고, 전파 관리, 항공안전, 치안, 재난 대응 등 다양한 기능을 담당하는 기관 간 협력이 필수적이다. 이에 따라 본 연구에서는 드론 위협 대응 과정에서 역할과 관여 수준에 따라 직접 대응 단체와 간접 대응 단체로 구분하여 정리하였다.

○ 직접 대응 단체

- 송출·전파 인프라 운영기관(KT스카이라이프 등): 송신소·중계망 운영 및 장애 대응 협력
- 전파관리소(과학기술정보통신부 소속): 전파 혼신 감시 및 불법 전파 사용에 대한 행정 조치
- 경찰청·지방경찰청: 드론 침입·불법비행 대응 및 현장 조치·수사
- 군(공군·방공부대 등): 군사·고도 제한 공역 내 드론 위협 대응 및 공역 통제 지원
- 국가·지역 대테러센터: 테러 연관 드론 위협 판단 및 관계기관 대응 조정
- 소방·재난안전 기관: 방송시설 피해 발생 시 재난 대응 및 안전 조치 연계

○ 간접 대응 단체

- 지방자치단체: 방송국 주변 공역 관리, 불법 드론 계도·단속 지원, 지역 재난관리 체계와 연동
- 규제·정책기관(방송통신위원회·과학기술정보통신부·국토교통부): 방송서비스·전파·항공안전 등 제도적 규율 담당
- 민간 협력업체(보안·안티드론·시설관리): 탐지·관제·물리보안 등 기술·운영 지원 역할 수행

이러한 구분은 이후 대응 시나리오 설계와 기관 간 역할 분담을 명확히 하기 위한 기준으로 활용된다.

4. 위험 기준(Risk Criteria) 설정

가. 위험 기준 설정 방법

위험 기준(Risk Criteria)은 위험의 중요성을 판단하고 대응 방향을 결정하기 위해 사전에 마련하는 평가 기준이다. ISO 31000은 조직의 목표에 비추어 수용 가능한 위험 수준을 명확히 정의할 것을 요구하며, 이는 위험 평가에서 의사결정의 기준점으로 활용된다. 또한 본 연구에서는 외부 정책연구의 특성을 고려하여, 공개 정보와 제도적 기준을 바탕으로 설정 가능한 항목을 중심으로 위험 기준을 구성하였다. 위험 기준을 설정할 때 고려해야 할 항목은 <표 3-3>과 같다.

〈표 3-3〉 위험 기준 설정에 필요한 주요 항목

구 분	주요 내용	적용 범위
불확실성 파악	결과와 목표에 영향을 미치는 불확실성은 어떻게 정의할 것인가?	Y
결과·가능성 기준	영향과 발생가능성을 어떤 척도와 기준으로 정의할 것인가?	Y
시간 요소 파악	위험의 발생·영향이 시간에 따라 어떻게 변화하는가?	Y
측정의 일관성	위험 평가 지표와 측정 방식의 일관성은 어떻게 유지할 것인가?	Y
위험 수준 결정	위험 수준을 어떤 방식과 기준으로 산정할 것인가?	Y
복합 위험 고려	복수 위협의 동시·연속 발생을 어떻게 반영할 것인가?	Y
조직 역량	조직의 자원·역량은 위험 기준에 어떤 제약을 부여하는가?	N

자료: ISO 31000:2018을 참고하여 본 연구에 맞게 재구성

나. 방송시설 대상 위험 기준 설정

본 연구는 방송시설을 대상으로 한 위험 기준의 개념적 구조와 판단 원칙을 중심으로 서술한다. 이에 따라 실제 위험 평가에 활용되는 세부 점수 구간, 등급 정의, 산정 공식 및 기준표는 운용 단계에서의 활용성과 재현성을 고려하여 부록의 ‘1. 방송시설 대상 위험 기준 산정’에 별도로 정리하였다. 본문에서는 위험 기준 설정의 논리적 틀과 판단 체계를 제시하고, 구체적인 수치 기준과 산정 예시는 부록을 통해 확인할 수 있도록 구성하였다.

1) 불확실성 파악

방송시설을 대상으로 한 드론 위협은 기체의 성능, 운용 방식, 주변 환경, 방어 여건 등에 따라 매우 다양한 양상으로 나타난다. 동일한 드론이라 하더라도 운용 목적과 환경 조건에 따라 위협 수준과 피해 가능성이 크게 달라질 수 있으므로, 위험 평가에 앞서 위협 상황을 구성하는 주요 불확실 요소를 체계적으로 파악할 필요가 있다.

이에 본 연구에서는 드론 자체의 특성과 운용 조건, 그리고 방송시설이 놓인 환경적 요인을 중심으로 불확실성을 다음과 같이 구분하여 정리하였다.

○ 드론 관련 정보

- 드론의 크기(소형・중형・대형)
- 드론의 항법 방식(RF 조종, GNSS 기반, 자율비행 등)
- 드론의 운용 형태(단독 운용, 군집 운용)
- 드론 통신 신호 특성(RF 출력 수준, 링크 안정성 등)
- 사용 주파수 대역(허가・비허가 대역, 채널 점유 특성)
- 기체 탑재물 여부(페이로드 존재 및 유형)
- 공격 수행에 요구되는 기술적 진입장벽
- 공격 자원(기체・장비・기술)의 획득 난이도

○ 환경 정보

- 시설 인근 2차 피해 위험 구역(낙하물, 하드킬 대응 시 영향 범위)
- 전파 혼신에 민감한 설비 또는 구역 존재 여부
- 지형・구조물 특성(건물 밀집도, 음영구역, 반사 환경)
- 인구 밀집도 및 안전 위험 수준
- 방송시설 방어체계 현황(탐지・무력화 장비 구성)
- 방어 구역 및 설비 정보의 외부 노출 수준
- 방어 구역의 물리적 접근성

이와 같이 정리된 불확실성 요소들은 이후 피해 영향도(Impact)와 발생 가능성

(Likelihood)을 판단하기 위한 기초 정보로 활용된다.

2) 결과 및 가능성 기준

○ 피해 영향 기준

드론 위협으로 인해 방송시설이 받게 되는 영향은 단일 요인만으로 설명하기 어렵다. 방송서비스의 연속성은 전파 혼신, 장비 손상, 물리적 충돌 등 다양한 형태의 자극에 의해 저해될 수 있으며, 그 결과는 다음과 같이 나타날 수 있다.

- 방송송출 품질 및 연속성에 직접적인 영향을 미치는 서비스 중단 영향(DoS, Denial of Service)
- 설비 손상, 2차 피해, 안전사고로 이어질 수 있는 안전 영향

두 영향은 독립적이면서도 실제로는 복합적으로 발생할 수 있으므로, 이를 병렬적으로 고려하여 방송서비스와 시설 안전에 대한 피해 수준을 종합적으로 분석한다.

○ 피해 발생 가능성 판단 요소

방송시설을 대상으로 한 드론 위협은 단순 접근 여부만으로 피해 발생 가능성을 판단하기 어렵고, 공격 주체의 역량, 수단 확보성, 표적 정보 노출, 물리적 접근 여건, 그리고 시설의 탐지·대응체계 수준 등 복합 요인의 영향을 받는다. 이에 본 연구에서는 피해 발생 가능성을 공격이 현실에서 실행될 수 있는 조건의 성숙도 관점에서 정의하고 다음 요소를 기준으로 평가한다

- 공격 수행의 기술적 수행 용이성
- 공격 수단의 확보 용이성
- 표적 정보의 노출 수준
- 물리적 접근 조건 및 주변 환경
- 시설의 탐지·대응체계 수준

본 연구는 상기 요소를 종합하여 피해 발생 가능성을 단계적으로 판단하며, 이를 조건 기반 가능성 평가로 정의한다.

3) 시간 요소 파악

드론 위협으로 인한 방송시설의 피해는 위협의 지속 시간과 피해 이후 복구 소요 시간에 따라 영향 범위와 위험 수준이 크게 달라질 수 있다. 특히 방송서비스는 시간에 민감한 공공 서비스이므로, 피해가 장시간 지속되거나 복구가 지연될 경우 위험 수준이 비선형적으로 확대되는 특성을 가진다. 이에 본 연구에서는 다음 두 가지 시간 요소를 중심으로 평가한다.

○ 위협 지속 시간

- 드론의 체공 또는 침입 시간이 길어질수록 방송송출 품질 저하, 서비스 중단, 인프라 손상 및 2차 피해로 이어질 가능성이 점진적으로 증가하며, 일정 임계 시간을 초과할 경우 피해 영향이 급격히 확대될 수 있음

○ 복구 소요 시간

- 위협 종료 이후 방송 설비 및 서비스가 정상화되기까지 소요되는 시간으로, 복구가 지연될수록 방송 중단 범위와 사회적 영향이 누적되어 전체 위험 수준을 증대시키는 주요 변수로 작용함

본 연구는 상기 시간 요소를 피해 영향 및 발생 가능성 평가 과정의 조정 변수로 반영하여 위험 수준을 산정한다.

4) 측정의 일관성

드론 위협은 사례가 제한적이고 변동성이 크기 때문에, 평가 결과의 수치가 동일하게 반복되는 ‘절대적 일관성’ 확보에는 한계가 있다. 이에 본 연구에서의 측정의 일관성은 모든 평가 대상에 동일한 기준과 절차를 적용하여 상대적 위험 수준을 비교할 수 있도록 하는 것으로 정의한다. 본 연구에서는 사전에 정의한 영향도(Impact)와 발생 가능성(Likelihood) 기준을 모든 평가 대상에 동일하게 적용하여 평가의 단순성과 적용의 명확성을 확보하였다. 이에 따라 다음의 원칙을 적용하였다.

○ 측정의 일관성 확보 원칙

- 영향도(Impact)는 최대 10점의 범위 기준에 따라 산정
- 발생 가능성(Likelihood)은 동일한 판단 요소와 등급 정의를 적용하여 최대 10점의 범위 기준에 따라 산정
- 모든 시설과 위협 시나리오는 동일한 평가 절차를 통해 비교·분석
- 평가 결과는 절대값이 아닌 상대적 위험 수준 비교를 중심으로 해석

산정된 영향도와 발생 가능성은 결합되어 종합적인 위험 수준(Risk Level)을 산정한다.

5) 복합 위험 가능성

드론 위협은 단일 침입에 한정되지 않으며, 복수의 위협이 동시에 또는 연속적으로 발생할 수 있다. 이에 본 연구는 방송시설 자산별·위협 유형별로 위험을 개별 식별·평가하는 방식을 적용한다.

○ 복합 위험성 고려 원칙

- 모든 위협은 특정 자산 또는 자산군에 귀속하여 개별 위험으로 정의
- 동일 시간대에 복수 위협이 발생하더라도, 각 위협은 독립된 영향도 및 발생 가능성 기준으로 평가
- 복합 상황은 개별 위험의 단순 합산이 아닌, 운영·대응 측면에서 관리 대상이 되는 동시 발생 시나리오로 해석

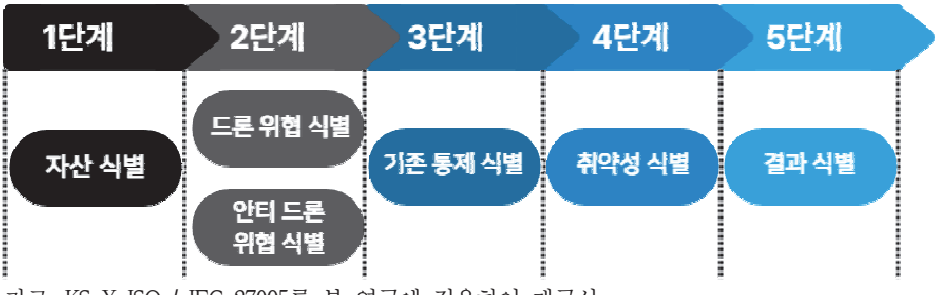
이를 통해 복합 위협 상황에서도 자산별 위험 수준과 대응 필요성을 명확히 식별한다.

제 3 절 방송시설 위험 식별(Risk Identification) 단계

1. 방송시설 위험 식별 개요

위험 식별은 방송시설을 대상으로 드론 위협과 안티드론 운용 과정에서 발생할 수 있는 부수적 위험 요인을 체계적으로 도출하는 절차이다. 본 연구는 KS X ISO/IEC 27005에서 제시하는 자산 식별, 위협 식별, 기존 통제 파악, 취약성 식별, 결과 식별의 단계적 구조를 적용하되, 드론 기반 공격과 안티드론 운용에서 발생할 수 있는 특수한 위험 요소를 중심으로 분석 절차를 구성하였다. 본 연구의 위험 식별 절차는 [그림 3-2]와 같다.

〔그림 3-2〕 본 연구의 위험 식별(Risk Identification) 흐름도



자료: KS X ISO / IEC 27005를 본 연구에 적용하여 재구성

위험 식별 단계는 본 연구에서 설정한 평가 범위 내에서 어떠한 자산이 보호 대상이 되는지, 그리고 해당 자산에 어떠한 형태의 드론 위협 및 안티드론 운용 관련 부수 위험이 존재하는지를 체계적으로 정리하는 출발점에 해당한다. 특히 방송시설은 송출·수신·제어·운영 기능이 복합적으로 결합된 구조를 가지므로, 단일 위협만을 전제로 한 단순 식별 방식으로는 실제 위험 구조를 충분히 반영하기 어렵다. 이에 따라 본 연구에서는 자산, 위협, 취약성, 결과 간의 인과 관계를 구조적으로 연결하는 방식으로 위험 식별 절차를 구성하였다. 위 흐름도를 구성하는 세부 단계는 각 절차의 목적과 적용 방향에 따라 <표 3-4>와 같이 정리된다.

〈표 3-4〉 위험 식별 세부 단계

단 계		정 의	본 연구의 적용 방향	산출물
자산 식별		보호 대상 자산을 식별하고 범주화	드론·안티드론 영향 범위 내 주요 설비·시스템·인력 중심으로 자산 구분	자산 목록
위협 식별	드론	드론으로 인해 발생하는 직접적 위협 도출	침입, 충돌, 전파 간섭 등 드론 행위 기반 위협을 파악	드론 위협 목록
	안티 드론	대응 과정에서 발생하는 2차 위험 도출	전파 혼신, 오탐·미탐, 장비 오작동 등 부수적 위험을 확인	안티 드론 위협 목록
기존 통제 식별		현재 적용 중인 보호 조치 확인	탐지·감시 체계, 절차, 물리적 보호 등 통제 수준을 점검	기존 통제 현황
취약성 식별		위협이 현실화될 수 있는 약점 확인	탐지 한계, 절차 미비, 장비 성능 한계 등 취약 요소를 검토	취약성 목록
결과 식별		위협 발생 시 피해 유형 정의	사고 시나리오에 대한 방송 중단, 설비 손상, 전파 혼신 등 영향 유형을 정리	시나리오 기반 결과

자료: KS X ISO/IEC 27005를 본 연구에 적용하여 재구성

위와 같은 절차를 기반으로 식별된 정보는 이후 위험 분석과 위험 평가 단계에서 활용된다.

2. 자산 식별 및 정의

가. 자산 식별 기준

드론 기반 위협과 안티드론 대응은 기존 방송시설 위험관리 체계와 성격이 상이하므로, 어떤 구성요소를 '자산'으로 간주할 것인지에 대한 기준을 명확히 설정할 필요가 있다. 이는 단순히 설비를 나열하는 것이 아니라, 드론 공격 또는 안티드론 대응이 방송서비스에 어떠한 영향을 미칠 수 있는지를 중심으로 자산의 범위를 규정하는 과정이다. 본 연구에서는 다음의 세 가지 관점을 기준으로 방송시설 자산을 식별하였다.

첫째, 드론 공격(재밍·침입·충돌 등)이 직접적으로 영향을 미칠 수 있는 자산이다. 드론은 전파 방출, 저고도 접근, 물리적 충돌 등의 방식으로 방송시설에 즉각적 피해를 줄 수 있으므로, 방송송출 및 전송 기능을 수행하는 자산은 주요 보호 대상으로 분류된다.

둘째, 안티드론 대응 과정에서 간접적·2차적 영향을 받을 수 있는 자산이다. 전파 기반 대응(재밍, 스푸핑, 탐지 신호 송출)이나 물리적 대응 과정은 방송시설의 전파 환경 및 인

접 설비에 부수적 영향을 미칠 수 있으므로, 안티드론 운용과 상호작용하는 자산 역시 위험 분석 대상에 포함된다.

셋째, 드론 위협 또는 안티드론 대응이 현실화될 경우 방송서비스의 연속성에 중대한 영향을 미칠 수 있는 자산이다. 직접적인 물리 피해가 발생하지 않더라도, 해당 자산의 장애는 방송 중단, 전파 혼신 확대, 재난방송 수행 실패 등으로 이어질 수 있으므로 보호 대상 자산으로 식별된다.

이러한 기준을 종합하여 본 연구에서는 방송시설 자산을 유형 자산과 무형 자산으로 구분하고, 각 자산을 개별 식별이 가능한 단위로 정의하였다.

다. 방송시설 자산 정의 및 체계화

방송시설을 대상으로 한 드론 위협과 안티드론 대응 위험을 분석하기 위해서는, 보호 대상이 되는 자산의 범위를 먼저 정의할 필요가 있다. 그러나 방송시설은 국가중요시설로서 세부 장비 구성 및 배치 정보의 공개가 제한되므로, 개별 장비 단위로 자산을 세분화하여 분류하기에는 현실적인 한계가 존재한다.

이에 본 연구에서는 “드론 또는 안티드론 운용에 의해 실제로 위협받을 수 있는 지점이 어디인가?” 라는 관점에서 자산 범위를 재정렬하였다. 그 결과, 방송시설 자산은 유형 자산과 무형 자산의 두 범주로 구분하였다.

유형 자산은 방송 신호의 생성・제어・송수신이 이루어지는 시설・공간・설비로서, 드론의 물리적 침입・충돌 또는 전파 기반 교란이 직접적인 피해로 이어질 수 있는 대상이다. 무형 자산은 방송서비스 제공의 전제가 되는 전파 자원으로, 물리적 손상이 없더라도 혼신・점유・간섭이 발생할 경우 즉각적인 서비스 장애로 연결될 수 있는 대상이다.

무형 자산은 물리적 형태는 없으나, 방송서비스 제공의 전제가 되는 전파 자원 및 주파수 대역을 의미한다. 무형 자산은 임의적 범위 설정을 방지하기 위해 「2025 대한민국 주파수 분배표」를 기준으로 현재 방송에 사용 중인 대역만을 선별하여 정의하였으며, 세부 주파수 범위는 <표 3-5> 및 <표 3-6>에 제시된 분배 현황을 근거로 한다.

〈표 3−5〉 방송에 사용 중인 중파, 단파 대역

구분	주파수 범위	용도	현재 사용 여부
중파(MF)	526.5 kHz ~ 1606.5 kHz	표준방송(AM 라디오)	사용 중
단파(HF)	5950 ~ 6200 kHz	국제 단파방송	사용 중
	7200 ~ 7450 kHz	국제 단파방송	사용 중
	9500 ~ 9900 kHz	국제 단파방송	사용 중
	11650 ~ 12050 kHz	국제 단파방송	사용 중
	13600 ~ 13800 kHz	국제 단파방송	사용 중
	15100 ~ 15600 kHz	국제 단파방송	사용 중
	17550 ~ 17900 kHz	국제 단파방송	사용 중
	21450 ~ 21850 kHz	국제 단파방송	사용 중
	25670 ~ 26100 kHz	국제 단파방송	사용 중

자료: 2025 대한민국 주파수 분배표

〈표 3−6〉 방송에 사용 중인 초단파, 극초단파, M/W 대역

구분	주파수 범위	용도	현재 사용 여부
초단파 (VHF)	54 ~ 72 MHz	아날로그 TV (CH 2~4)	미사용
	76 ~ 88 MHz	아날로그 TV (CH 5~6)	미사용
	88 ~ 108 MHz	FM 라디오 방송	사용 중
	174 ~ 216 MHz	아날로그 TV (CH 7~13)	미사용
극초단파 (UHF)	470 ~ 698 MHz	지상파 TV 방송 (UHF CH 14-51)	사용 중
	698 ~ 806 MHz	TV(과거), 현재 이동통신(LTE/PS-LTE)	방송 미사용
마이크로파 (M/W)	2.4 GHz, 5 Ghz ISM 대역	방송 설비 운용 및 제어 신호 사용	사용 중
	1700 MHz ~ 1710 MHz	프로그램 중계 링크	사용 중
	4400 MHz ~ 4500 MHz	TV 이동 중계 링크	사용 중
	6425 MHz ~ 6605 MHz, 6765 MHz ~ 6945 MHz, 7725 MHz ~ 8275 MHz, 8275 MHz ~ 8500 MHz	방송 고정 중계 링크	사용 중

자료: 2025 대한민국 주파수 분배표

앞서 설정한 자산 식별 기준에 따라, 본 연구에서 정의한 방송시설 자산은 <표 3−7>과 같다. 각 자산은 드론 위협 및 안티드론 대응과의 관계를 기준으로 자산 번호(A-01~A-16)

를 부여하여 관리하며, 이후 위협 식별, 위험 분석, 위험 평가 단계에서 공통 기준으로 활용된다.

〈표 3-7〉 방송시설 자산 정의

대분류	중분류	자산명	내용	자산 번호
유형 자산	연주소	주조정실	방송 편성 및 송출을 통합 제어하는 핵심 운용 공간	A-01
		부조정실	제작·송출 보조 제어를 수행하는 연계 운용 공간	A-02
		연주소 송신 시설	연주소에서 송신소·중계소로 방송 신호를 전달하기 위한 송신 링크 설비와 송신 안테나 및 지지 구조물을 포함하는 전파 송신체계	A-03
		연주소 주변 시설	연주소 인근 주거·상업·공공시설 등 외부 영향 대상	A-04
	송·중계소	송·중계소 수신 시설	연주소 또는 상위 중계소로부터 방송 신호를 수신하는 설비 및 수신 안테나·연계 설비	A-05
		송·중계소 송신 시설	수신된 방송 신호를 증폭·제어하여 송신하고, 출력과 송신 품질을 관리하는 설비 및 송신 안테나·지지 구조물	A-06
무형 자산	MF	AM 방송서비스	526.5 kHz ~ 1606.5 kHz 중파 대역 방송 신호	A-07
	HF	국제 단파 방송	6 MHz ~ 26 MHz 단파 대역 방송 신호	A-08
	VHF	FM 방송	30 MHz ~ 300 MHz 초단파 대역 방송 신호	A-09
		DMB 방송	174 MHz ~ 216 MHz 이동 수신 방송 신호	A-10
	UHF	디지털 TV 방송	470 MHz ~ 698 MHz ATSC 1.0 방송 신호	A-11
		UHD 방송	470 MHz ~ 698 MHz ATSC 3.0 방송 신호	A-12
	ISM	방송 설비 운용 및 제어 신호	2.4 GHz / 5 GHz ISM 대역 운용 신호	A-13
	M/W	프로그램 중계 링크	1700 MHz ~ 1710 MHz 대역	A-14
		TV 이동 중계 링크	4400 MHz ~ 4500 MHz 대역	A-15
		방송 고정 중계 링크	6425 MHz ~ 6605 MHz, 6765 MHz ~ 6945 MHz, 7725 MHz ~ 8275 MHz, 8275 MHz ~ 8500 MHz 대역	A-16

한편, 본 연구에서 직접적인 위험 평가 대상에 포함되지 않은 자산은 그 중요성을 배제하는 것이 아니라, 드론 위협이 현실화될 경우 서비스 장애의 파급, 복구 과정, 운영 연속성에 영향을 미칠 수 있는 요소로서 자산 체계 내에 유지한다. 이러한 자산은 향후 보다 확장된 위험 평가 또는 후속 연구에서 심층적으로 분석될 수 있다.

3. 위협 식별

가. 위협 행위자 식별

위협이란 식별된 자산에 해를 가하거나 손실을 유발할 수 있는 모든 행위를 의미하며, 이는 악의적인 의도를 가진 공격뿐 아니라 실수, 오작동, 부수적 피해 형태로 발생하는 상황까지 포함한다. 일반적으로 자산에 위협을 가하는 행위자는 인간과 비인간으로 구분될 수 있으며, 인간은 다시 내부자와 외부자로, 비인간은 기술・장비・환경 요인 등을 포함한다.

본 연구에서는 방송시설 보호 관점에서 분석 대상을 비인간 행위자 중 드론을 중심으로 한 위협으로 한정한다. 이는 드론 자체에 의한 직접적 위협뿐 아니라, 드론 대응 과정에서 운용되는 안티드론 시스템으로 인해 발생할 수 있는 부가적・2차적 위협까지 포함하는 개념이다. 따라서 본 연구에서의 위협 행위자는 크게 드론과 안티드론 시스템으로 구분된다.

1) 위협 행위자, 드론

드론은 접근 용이성, 기동성, 적재 능력, 전파 활용 특성으로 인해 방송시설에 다양한 형태의 위협을 유발할 수 있다. 본 연구에서는 “어떤 드론이 위협 주체가 될 수 있는가?”를 명확히 하기 위해, 드론 유형을 다음 세 가지 기준에 따라 분류하였다.

① 드론에 적재 가능한 페이로드(Payload)에 따른 분류

이는 드론이 자산에 미칠 수 있는 물리적 피해의 잠재 규모와 직접적으로 연관되는 요소로, 충돌, 자폭, 투하 등 물리적 공격 시나리오의 영향 범위를 판단하기 위한 기준이다. 본 연구에서는 드론을 소형・중형・대형 드론으로 구분하였으며 자세한 내용은 <표 3−8>과 같다.

〈표 3-8〉 페이로드 적재량에 따른 드론의 유형 분류

드론 유형	종류	적재량
소형 드론	FPV 자작 드론 상용 DJI 드론	2.8kg ~ 35.2kg
중형 드론	농업용 방제 드론 대형 물류 드론	35.3kg ~ 67.6kg
대형 드론	고정익 드론	67.7kg ~ 100kg

자료: 드론위협 대응을 위한 국가중요시설의 방호 전략 연구 재구성

이와 같은 분류는 단순한 기체 크기 구분이 아니라, 어떤 수준의 물리적 피해가 현실적으로 발생 가능한지를 판단하기 위한 기초 정보로 활용된다. 예를 들어 소형 드론이라 하더라도 고속 FPV 형태로 운용될 경우 충돌 위험은 충분히 치명적일 수 있으며, 중·대형 드론은 설비 파손이나 인명 피해 가능성을 내포한다.

② 드론의 항법 및 제어 방식에 따른 분류

드론의 제어 방식은 탐지 가능성, 대응 시간, 대응 수단의 선택에 직접적인 영향을 미치며, 이는 곧 위협의 실현 가능성과 피해 양상으로 이어진다. 본 연구에서는 드론의 항법 방식을 RF 제어형, 유선 제어형, 자율비행형, 고속 기동형으로 구분하였고, 자세한 내용은 〈표 3-9〉와 같다.

〈표 3-9〉 드론 항법 방식에 따른 드론의 유형 분류

드론 유형	종류	설명
RF 제어형	일반 상용 드론	조종자와 드론 간의 주파수 통신을 통한 비행 드론
유선 제어형	광 통신 드론	물리적 광케이블을 통해 제어
자율비행 형	전파 침묵형 드론	통신 없이 전파 '침묵(Radio Silence)' 상태 침투 드론
고속 기동형	소형 FPV 드론	아날로그 비디오 신호를 사용하며 시속 100km 이상의 고속으로 이동

RF 제어형 드론은 전파 기반 탐지·무력화가 가능한 반면, 자율비행형 드론이나 전파 침묵 상태로 침투하는 기체는 탐지 실패 가능성을 높인다. 또한 고속 기동형 FPV 드론은 대응 시간을 극단적으로 단축시켜, 물리적 충돌 위험을 증대시키는 특성을 가진다. 이러한 항법 방식의 차이는 동일한 자산이라 하더라도 위협의 성격과 대응 난이도를 달라지게 만드는 핵심 요소이다.

③ 드론의 운용 형태에 따른 분류

드론이 단독으로 운용되는지, 혹은 다수의 드론이 동시에 침투하는 군집 형태로 운용되는지는 위협의 범위와 파급성에 큰 차이를 만든다. 본 연구에서는 운용 형태를 단독 비행과 군집 비행으로 구분하였고, 이는 <표 3-10>과 같다.

〈표 3-10〉 드론 운용 형태에 따른 분류

드론 유형	설명
단독 비행	1대 침투
군집 비행	다수 동시 침투

군집 비행은 단일 자산에 대한 반복 공격뿐 아니라, 복수 자산에 대한 동시 또는 연쇄적 위협을 가능하게 하며, 방어 자원의 분산을 유도함으로써 전체 방어 효율을 저하시킬 수 있다. 따라서 운용 형태는 위협 시나리오의 복합성 및 영향 확산 가능성을 판단하는 중요한 기준으로 작용한다.

다만 드론의 실제 운용 방식과 조합 가능한 위협 시나리오는 매우 다양하며, 모든 유형과 조합을 개별적으로 분석하는 것은 본 연구의 범위와 목적을 넘어서는 한계가 있다. 따라서, 본 연구에서는 드론 기반 위협 행위자를 다음과 같이 고정해서 정의한다.

○ 본 연구의 드론에 대한 위협 행위자 한정

- 대형 드론
- RF 제어형 항법 방식
- 단독 비행 형태

이는 방송시설 자산에 대해 현실적으로 가장 큰 물리적·운영상 영향을 미칠 수 있는 보수적 가정을 적용한 것으로, 위험을 과소평가하는 것을 방지하고 정책·운용 관점에서 대응 필요성이 높은 상황을 우선적으로 분석하기 위한 접근이다. 소형 드론, 자율비행형 또는 전파 침묵형 드론, 군집 비행 형태 등 기타 조합에 따른 위협 가능성은 향후 세부 기술 검증 및 실증 연구 단계에서 추가적으로 고려될 필요가 있다.

2) 위협 행위자, 안티드론 시스템

안티드론 시스템은 드론 위협을 탐지하고 무력화하기 위한 방어 수단이지만, 운용 방식과 기술적 특성에 따라 방송시설 자산에 새로운 위험을 유발할 수 있다. 특히 방송시설은 전파 기반 서비스와 설비에 대한 의존도가 높기 때문에, 안티드론 시스템의 전파 방출 여부와 물리적 대응 방식은 위협 행위자로서 별도의 분석이 필요하다. 이에 따라 본 연구에서는 안티드론 시스템의 탐지 단계와 무력화 단계에서 방송시설 자산에 영향을 미칠 수 있는 위협 특성을 중심으로 분석하였다.

① 탐지 유형에 따른 안티드론 시스템의 위협

안티드론 탐지 시스템의 모든 탐지 방식이 방송시설 자산에 동일한 수준의 위험을 초래하는 것은 아니다. 방송시설의 전파 운용 특성과의 상호작용이 위협 판단의 핵심 기준이 된다. RF 수신 기반 탐지와 EO/IR 기반 탐지는 전파 방사를 수반하지 않는 수동적 방식이므로 방송시설 자산에 대한 직접적 위험이 제한적인 반면, 레이다 기반 탐지는 고출력 전파 방사를 수반하여 방송 송수신 설비 및 인접 전파에 혼신을 유발할 가능성이 존재한다. 이에 탐지 유형에 따른 방송시설 위협 여부를 <표 3-11>과 같이 구분하였다.

〈표 3-11〉 탐지 유형에 따른 안티드론 시스템의 위협

탐지 유형	방송시설 위협 여부	비고
RF 탐지	매우 낮음	수동 수신 방식, 전파 방사 없음
EO/IR 탐지	매우 낮음	전파 영향 없음
음향 탐지	제외	실질적 운용 한계
레이다 탐지	높음	고출력 전파 방사, 혼신 가능성

② 무력화 방식에 따른 안티드론 시스템의 위협

안티드론 무력화 시스템은 탐지된 드론을 제거 또는 통제하기 위한 적극적 대응 수단으로, 물리적 파괴를 수반하는 하드킬 방식과 전파·신호 기반의 소프트킬 방식으로 구분된다. 이러한 무력화 기술은 드론 위협을 제거하는 동시에, 방송시설 자산에 직접적 또는 간접적인 영향을 미칠 수 있는 잠재적 위험 요인으로 작용한다.

소프트킬 방식은 송출 주파수, 중계 링크, 설비 제어 신호 등에 영향을 미칠 수 있으며, 하드킬 방식은 낙하물·파편·충돌 등에 따른 2차 피해를 유발할 가능성이 존재한다. 이에 따라 본 연구에서는 무력화 방식에 따른 안티드론 시스템의 분류를 <표 3-12>와 같이 구분하였다.

〈표 3-12〉 무력화 방식에 따른 안티드론 시스템의 위협

유형	종류		설명	위협 여부
하드킬	레이저		고출력 레이저로 파괴	높음
	HPM		고출력 마이크로파로 파괴	높음
	그물		발사형 그물로 비행 불능	높음
	요격 드론		직접 접근하여 충돌 파괴	높음
소프트킬	단순	전방위 재밍	광역 전파 방해	높음
		지향성 재밍	특정 방향 전파 방해	높음
		GPS 스푸핑	위성항법(GNSS) 신호를 기만	높음
	정밀	스마트 재밍	선택적 주파수/시간 방해	매우 낮음
		정밀통제형	드론의 제어권을 탈취하여 통제	매우 낮음

나. 위협의 분류

위협이란 식별된 자산에 피해를 유발하거나, 정상적인 기능 수행을 저해할 수 있는 모든 잠재적 원인을 의미한다. 즉, 본 연구에서의 위협 분류는 “어떤 자산이 위험에 노출되는가”가 아니라, “어떤 종류의 부정적 사건이 발생할 수 있는가”를 정의하는 과정이다. 이는 이후 위협 시나리오 구성과 영향도·발생 가능성 평가의 기준이 되므로, 위협의 성격을 명확히 구분하는 것이 중요하다.

이에 따라 본 연구에서는 방송시설 보호 관점에서 드론 및 안티드론과 관련된 위협을

다음 세 가지 유형으로 구분하였다.

첫째, 의도적인 적대적 공격 위협은 방송시설에 대한 명확한 피해 의도를 가지고 수행되는 행위로, 자산 파괴, 방송 중단, 인명 피해 등을 직접적인 목표로 한다.

둘째, 우발적 사고 위협은 명확한 공격 의도 없이 발생하는 드론의 침범이나 충돌 등으로, 방송 운영에 혼선이나 간접적 피해를 유발할 수 있는 유형이다.

셋째, 안티드론 운영에 따른 부수적 피해 위협은 드론 대응 과정에서 사용되는 탐지·무력화 기술로 인해 전파 혼신, 설비 오작동, 낙하물 피해 등이 발생하는 경우를 포함한다.

이러한 분류 기준에 따라 본 연구에서 정의한 위협 유형은 <표 3-13>과 같다.

〈표 3-13〉 방송시설의 위협 리스트

유형	위협 ID	설명	행위자	지속시간	범위
적대적 공격	T-01	자폭 및 폭탄 투하	드론	순간적	핵심 시설
	T-02	위협물 투하	드론	수 시간 ~ 수 주	핵심 시설
	T-03	무장 난사 공격	드론	수 분 ~ 수십 분	인명
	T-04	불법 정찰 및 감시	드론	수 분 ~ 수 시간	핵심 시설
	T-05	사이버 공격	드론	수 분 ~ 수 시간	내부 통신망
우발적 사고	T-06	단순 침범	드론	수 분 ~ 수십 분	업무 혼선
	T-07	시설물 충돌	드론	순간적	핵심 시설
부수적 피해	T-08	전파 혼신	안티 드론	수 분 ~ 수십 분	주파수 스펙트럼
	T-09	고출력 전파 방사	안티 드론	순간적 ~ 수 분	송수신 시설
	T-10	요격 잔해 낙하	안티 드론	순간적	인명, 외부 시설
	T-11	요격으로 드론의 폭발물 낙하	안티 드론	순간적	인명, 외부 시설

한편, ‘T-09(고출력 전파 방사)’는 안티드론 무력화 과정에서 발생하는 고출력 전파가 방송시설 송·수신 설비에 직접적인 영향을 미칠 수 있는 위협 유형으로, 전파 출력 수준, 방사 패턴, 운용 시간 등 다수의 기술적 변수를 포함하여 검증이 요구되는 영역으로 판단된다. 이에 본 연구에서는 ‘T-09’을 위협 분류에는 포함하되, 시나리오 구성 및 위험 평가 대상에서는 제외하고, 향후 실증 또는 후속 정책 연구를 통해 별도로 검토할 필요가 있음을 명시한다.

4. 기존 통제 식별

본 연구에서는 방송시설의 기존 통제를 드론 위협을 전제로 설계된 체계로 간주하지 않고, 현재 운영 중인 보안·관리 체계가 드론 위협에 대해 어떠한 수준의 대응 여력을 갖는지를 식별하는 관점에서 정리하였다.

1) 연주소의 기존 통제 수준

연주소는 방송 신호의 생성·제어·링크 송신이 집중되는 핵심 시설로, 출입 통제, 경비 인력, CCTV 등 지상 기반의 물리적 보안 체계를 중심으로 관리되고 있다. 이러한 통제는 주로 출입 동선 관리와 내부 공간 보호를 목적으로 설계되어 있으며, 공중에서 접근하는 드론 위협을 직접적인 통제 대상으로 포함하는 구조는 제한적이다.

또한 주요 운용 공간과 핵심 설비가 건물 내부에 위치하는 특성상, 기존 통제는 건물 외곽과 내부 구역 보호에 초점을 둔 형태로 구성되어 있다. 이로 인해 연주소의 물리적 통제 환경은 지상 접근 관리에는 효과적으로 작동하나, 드론과 같은 공중 접근 위협에 대해서는 별도의 탐지·차단 체계가 전제되지 않은 구조적 특성을 가진다.

2) 송·중계소의 기존 통제 수준

송·중계소는 주로 산악 지역이나 고지대에 위치하여 지상 접근은 제한되는 반면, 공중에서 접근하는 드론에 대해서는 물리적 차폐나 구조적 통제 수단이 제한적인 환경을 가진다. 일부 시설은 군 보호구역 또는 군 감시 체계와 공간적으로 인접하거나 중첩되어 있으나, 이러한 통제는 지상 접근 및 인원 이동을 중심으로 설계된 체계로, 드론의 공중 접근

을 직접 통제하기 위한 목적과는 구분된다. 따라서 송·중계소의 기존 물리적 통제 환경은 지상 접근 관리에는 일정한 효과를 가지나, 드론 접근에 대해서는 별도의 고려가 필요한 구조적 특성을 가진다.

5. 취약성 식별

취약성 식별은 위협 행위가 발생할 경우 기존 통제 수준이나 자산의 구조적 특성으로 인해 피해가 확대·전이될 수 있는 약점을 도출하는 과정이다. 본 연구에서는 개별 장비 성능보다는 자산의 공간적 배치, 기능 집중 구조, 전파·네트워크 의존성, 전자기적 내구 특성을 중심으로 방송시설의 취약성을 분석하였다. 이에 따라 취약성은 외부 노출 취약성, 기능·전파 취약성, 사이버·네트워크 취약성, 전자기적 취약성, 파급 구조 취약성의 관점에서 종합적으로 식별하였다.

1) 외부 노출 자산 중심의 물리적 취약성

송신·수신 설비, 안테나, 철탑, 링크 설비 등은 옥외 설치 특성으로 인해 드론 접근·체공·충돌이 가능한 직접 노출 자산에 해당한다. 이러한 자산은 의도적 공격뿐 아니라 우발적 충돌이나 요격 잔해·낙하물에 의한 피해 가능성을 내포한다. 특히 안테나·수신 설비는 경미한 구조 변화만으로도 출력 저하나 수신 품질 악화가 발생할 수 있어, 물리적 손상 대비 기능적 영향이 크게 확대되는 특성을 가진다. 내부 운용 공간은 외부 노출 자산의 정상 동작을 전제로 기능이 유지되는 구조이다.

2) 연주소의 기능 집중 및 사이버·전파 취약성

연주소는 방송 신호 생성·제어·편성·송출 관리 기능이 집중된 핵심 거점으로, 기능 집중도가 높은 구조적 특성을 가진다. 이로 인해 내부 네트워크, 제어 시스템, 원격 관리 인터페이스에 대한 의존도가 높으며, 사이버·무선 기반 위협 발생 시 피해가 방송 전반으로 확산될 가능성이 존재한다. 또한 ISM 대역 활용 비중이 높은 환경 특성상, 전파 간섭이나 재밍, 안티드론 소프트킬 운용에 따른 비의도적 전파 영향이 내부 설비 운용에 영향을 미칠 여지가 있다.

3) 수신 장비의 취약성

방송 수신 장비는 약한 신호를 안정적으로 처리하기 위해 외부 전파 환경 변화에 민감하게 설계된 자산이다. 이에 따라 드론 대응 과정에서 운용되는 전파 기반 장비가 근접할 경우, 혼신이나 수신 품질 저하가 발생할 가능성이 존재한다. 이러한 영향은 즉각적인 고장보다는 감도 저하, 간헐적 오작동 등 장기적 품질 저하 형태로 나타날 수 있으며, 장애 원인 식별과 복구를 어렵게 만드는 요인으로 작용한다.

4) 송신탑・대형 구조물의 정찰 노출 취약성

송신탑 및 대형 안테나 구조물은 시각적 식별이 용이하여, 드론에 의한 정찰만으로도 위치・구조・접근 경로 정보가 비교적 쉽게 노출될 수 있는 자산이다. 이는 직접적인 피해가 발생하지 않더라도, 후속 위협 시나리오의 타게팅 정확도를 높이는 요인으로 작용할 수 있다. 특히 고정형 구조물은 위치 변경이 불가능하여 반복 정찰에 따른 정보 축적 가능성이 존재한다.

5) 송・중계소의 전송 구조 기반 전파 취약성

송・중계소는 방송 신호를 증폭・재송신하는 전파 방사 거점으로, 전송 경로 안정성이 핵심 요소이다. 산악지형 등으로 인해 무선 STL에 의존하는 경우 전파 간섭이나 재밍의 영향을 직접적으로 받는다. 중계소는 연쇄 구조를 가지는 경우가 많아, 단일 지점 장애가 다수 서비스로 확산될 가능성을 내포하며, 입지 특성상 복구 지연 가능성도 존재한다.

6. 결과 식별

결과 식별 단계는 앞서 수행한 자산 식별, 위협 유형 분류, 기존 통제 수준, 취약성 식별 결과를 종합하여 실제 방송시설 운용 환경에서 발생 가능한 위험 상황을 구체화하는 단계이다. 이는 개별 요소를 단순히 나열하는 것이 아니라, [자산-위협-통제-취약성]이 결합될 경우 현실에서 어떠한 위험이 발생하는지를 식별하는 절차에 해당한다.

본 연구에서는 위험을 추상적으로 정의하지 않고, 특정 자산을 중심으로 위협 행위가 발생했을 때 방송서비스, 설비, 인명 및 주변 환경에 초래되는 결과를 위협 시나리오

(Threat Scenario) 형태로 도출하였다. 위협 시나리오는 위험이 현실화되는 경로와 양상을 설명하는 분석 단위로서, 위험 식별 단계의 최종 산출물이다.

방송시설 대상 드론 위협은 전파 공간과 물리 공간을 동시에 활용한다는 특성을 가지며, 안티드론 시스템 운용 과정 역시 전파 방사, 요격, 차단 등으로 인해 부수적인 위험을 유발할 수 있다. 이에 따라 본 연구에서는 드론의 직접 위협과 안티드론 대응으로 인한 부수적 위험을 동일한 시나리오 체계 내에서 함께 고려하였다.

위협 시나리오는 자산 ID와 위협 ID를 결합하여 구성되며, 이를 통해 "어떤 자산이 어떤 위협에 노출될 경우 어떠한 결과가 발생하는가?" 를 명확히 표현한다. <표 3-14>은 이러한 기준에 따라 도출된 자산별 위협 시나리오를 정리한 것으로, 주요 방송 자산을 대상으로 드론 공격 및 안티드론 대응 과정에서 발생 가능한 대표적 위험 상황을 제시한다.

〈표 3-14〉 방송시설의 위협 시나리오

자산 ID	위협 ID	시나리오 ID	시나리오 설명	결과
주조정실 A-01	T-01	S-A01-01	자폭·폭탄 투하로 주조정실 구조 손상	방송송출 불능
	T-02	S-A01-02	화염병 등의 위협물 투하로 주조정실 화재 발생	방송 운용 불능
	T-03	S-A01-03	장착된 총기로 주조정실 인명 피해 발생	인명 피해
	T-04	S-A01-04	불법 정찰로 주조정실 위치·구조 노출	후속 공격 위험 증가
	T-05	S-A01-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송출 제어 시스템 침해	통신·제어 기능 상실
	T-06	S-A01-06	주조정실 인근 공역 단순 침범으로 업무 혼선	방송 운용 장애
	T-07	S-A01-07	주조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	시설 피해
부조정실 A-02	T-01	S-A02-01	자폭·폭탄 투하로 부조정실 구조 손상	방송 운용 불능
	T-02	S-A02-02	화염병 등의 위협물 투하로 부조정실 화재 발생	방송 운용 장애
	T-03	S-A02-03	장착된 총기로 부조정실 인명 피해 발생	인명 피해
	T-04	S-A02-04	불법 정찰로 부조정실 위치·구조 노출	후속 공격 위험 증가

	T-05	S-A02-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 방송 제작 및 제어 시스템 침해	통신·제어 기능 상실
	T-06	S-A02-06	부조정실 인근 공역 단순 침범으로 업무 혼선	방송 운용 장애
	T-07	S-A02-07	부조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	시설 피해
연주소 송신 시설 A-03	T-01	S-A03-01	자폭·폭탄 투하로 연주소 송신 시설 파괴	방송송출 불능
	T-02	S-A03-02	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	방송송출 장애
	T-03	S-A03-03	장착된 총기로 연주소 송신 설비 인근의 인명 피해 발생	인명 피해
	T-04	S-A03-04	불법 정찰로 연주소 송신 설비 위치·구조 노출	후속 공격 위험 증가
	T-05	S-A03-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	통신·제어 기능 상실
	T-06	S-A03-06	연주소 송신 시설 인근 공역 단순 침범으로 업무 혼선	방송 운용 장애
	T-07	S-A03-07	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	방송 품질 저하
	T-10	S-A03-10	요격 잔해가 연주소 송신 시설에 2차 피해	인명·시설 피해
	T-11	S-A03-11	요격 후 폭발물이 연주소 송신 시설에 2차 피해	인명·시설 피해
연주소 주변 시설 A-04	T-01	S-A04-01	자폭·폭탄 투하로 연주소 주변 시설 파괴	인명·시설 피해
	T-02	S-A04-02	화염병 등의 위협물 투하로 연주소 주변 시설 화재 발생	인명·시설 피해
	T-03	S-A04-03	장착된 총기로 연주소 주변 시설 인근의 인명 피해 발생	인명 피해
	T-04	S-A04-04	불법 정찰로 연주소 주변 시설 위치·구조 노출	후속 공격 위험 증가
	T-05	S-A04-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 주변 시설 민간 네트워크 사이버 침해	사회적 혼란
	T-06	S-A04-06	연주소 주변 시설 인근 공역 단순 침범으로 업무 혼선	사회적 혼란
	T-07	S-A04-07	연주소 주변 시설 인근 공역 비행, 시설 충돌로 부수적 피해	인명·시설 피해

	T-10	S-A04-10	요격 잔해가 연주소 주변 시설에 2차 피해	인명·시설 피해
	T-11	S-A04-11	요격 후 폭발물이 연주소 주변 시설에 2차 피해	인명·시설 피해
송·중계소 수신 시설 A-05	T-01	S-A05-01	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	방송송출 불능
	T-02	S-A05-02	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	방송송출 장애
	T-03	S-A05-03	장착된 총기로 송·중계소 수신 설비 인근의 인명 피해 발생	인명 피해
	T-04	S-A05-04	불법 정찰로 송·중계소 수신 설비 위치·구조 노출	후속 공격 위험 증가
	T-05	S-A05-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 수신 시스템 침해	통신·제어 기능 상실
	T-06	S-A05-06	송·중계소 수신 시설 인근 공역 단순 침범으로 업무 혼선	방송 운용 장애
	T-07	S-A05-07	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	방송 품질 저하
	T-10	S-A05-10	요격 잔해가 송·중계소 수신 시설에 2차 피해	인명·시설 피해
	T-11	S-A05-11	요격 후 폭발물이 송·중계소 수신 시설에 2차 피해	인명·시설 피해
송·중계소 송신 시설 A-06	T-01	S-A06-01	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	방송송출 불능
	T-02	S-A06-02	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	방송송출 장애
	T-03	S-A06-03	장착된 총기로 송·중계소 송신 설비 인근의 인명 피해 발생	인명 피해
	T-04	S-A06-04	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	후속 공격 위험 증가
	T-05	S-A06-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	통신·제어 기능 상실
	T-06	S-A06-06	송·중계소 송신 시설 인근 공역 단순 침범으로 업무 혼선	방송 운용 장애
	T-07	S-A06-07	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	방송 품질 저하
	T-10	S-A06-10	요격 잔해가 송·중계소 송신 시설에 2차 피해	인명·시설 피해
	T-11	S-A06-11	요격 후 폭발물이 송·중계소 송신 시설에	인명·시설

			2차 피해	피해
AM A-07	T-08	S-A07-08	AM 방송 전파 간섭	방송 품질 저하
국제 단파 A-08	T-08	S-A08-08	국제 단파 방송 전파 간섭	방송 품질 저하
FM A-09	T-08	S-A09-08	FM 방송 전파 간섭	방송 품질 저하
DMB A-10	T-08	S-A10-08	DMB 방송 전파 간섭	방송 품질 저하
디지털 TV A-11	T-08	S-A11-08	디지털 TV 방송 전파 간섭	방송 품질 저하
UHD A-12	T-08	S-A12-08	UHD 방송 전파 간섭	방송 품질 저하
방송 제어 A-13	T-08	S-A13-08	운용 및 제어 신호 전파 간섭	통신・제어 기능 상실
프로그램 중계 A-14	T-08	S-A14-08	프로그램 중계 링크 전파 간섭	방송송출 장애
이동 중계 A-15	T-08	S-A15-08	TV 이동 중계 링크 전파 간섭	방송송출 장애
고정 중계 링크 A-16	T-08	S-A16-08	방송 고정 중계 링크 전파 간섭	방송송출 장애

위협 시나리오 표에 제시된 영향도 항목은 각 시나리오가 방송서비스 연속성, 전파 운용, 물리적 설비 및 안전 측면에서 어떠한 유형의 피해로 이어질 수 있는지를 개략적으로 나타낸 것이다. 이를 통해 자산별・시나리오별 피해 양상의 차이를 직관적으로 확인할 수 있도록 하였으며, 동일한 위협이라 하더라도 자산에 따라 영향의 범위와 중대성이 달라질 수 있음을 함께 보여준다.

제 4 절 방송시설 위험 분석(Risk Analysis) 단계

1. 방송시설 위험 분석 개요

본 연구의 위험 분석은 KS X ISO/IEC 27005에서 제시하는 절차를 기반으로 하며, 위험 식별 단계에서 도출된 자산・위협・취약성・기존 통제 정보를 토대로 개별 위험의 영향을 평가하고 위험 수준을 산정하는 것을 목표로 한다. 본 개요에서는 위험 분석에 적용되는 정성적 분석과 정량적 분석의 특성을 비교하여 설명하고, 정성적 방식을 적용하는 이유를 제시한 후, 위험 수준 산정의 체계를 제시한다.

가. 정성적・정량적 분석 방법의 구분과 선택

KS X ISO/IEC 27005는 위험 분석 시 정성적 분석, 정량적 분석 또는 두 방식의 조합을 적용할 수 있도록 규정하고 있다. 정성적 분석과 정량적 분석의 주요 특징은 <표 3−15>와 같다.

〈표 3−15〉 정성적 위험 분석과 정량적 위험 분석의 비교

구 분	정성적 위험 분석	정량적 위험 분석
평가 방식	등급・서술 기반 평가 (높음・중간・낮음 등)	수치・확률・금액 등 계량 정보 기반 평가
요구 데이터	낮음 (전문가 판단・운영 경험 중심)	높음 (통계 자료・사고 데이터 필요)
장 점	빠르고 적용 용이, 초기・광범위 평가에 적합	객관성・정밀도 높음, 비용・효과 분석 가능
제 약	평가자의 주관 개입 가능, 등급 간 차이 모호	데이터 확보・산정 비용이 높고, 시간 소요가 큼
적용 상황	신기술, 사례 부족, 초기 평가 환경	충분한 사고 통계 및 수치 자료 존재

자료: KS X ISO/IEC 27005를 본 연구에 적용하여 재구성

드론 및 안티드론 분야는 기술 발전 속도가 빠르고 실제 사고 사례 및 통계 자료가 충분히 축적되지 않은 영역에 해당한다. 특히 방송시설과 같이 환경적・구조적 특수성이 큰

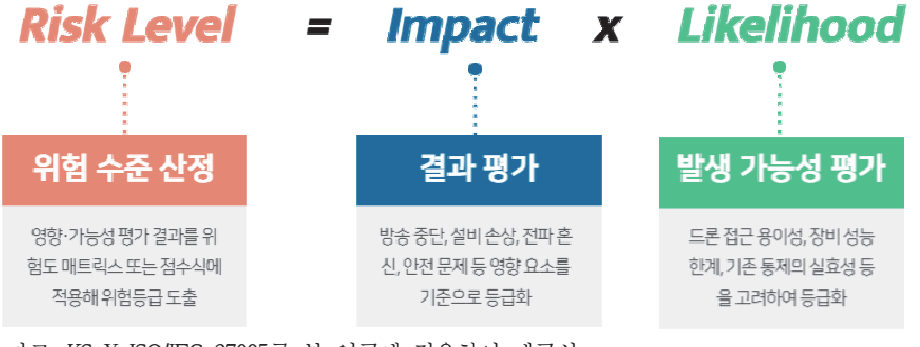
대상의 경우, 드론 침입, 전파 혼신, 오작동, 대응 과정에서의 부수적 영향 등에 대해 신뢰 가능한 발생 확률이나 피해 규모를 정량적으로 산정하는 데 한계가 존재한다. 또한 전파 방사 영향, 장비 내구 특성, 운용 방식 차이 등 계량에 영향을 미치는 변수가 매우 다양하여, 이를 포괄적으로 반영한 정량 분석은 본 연구의 범위를 넘어서는 것으로 판단하였다.

이에 따라 본 연구에서는 정량적 위험 분석은 적용하지 않고, 정성적 분석을 중심으로 위험의 유형, 발생 양상, 상대적 중요도를 평가하였다. 이러한 접근은 데이터가 제한적인 신기술 분야에 대해 KS X ISO/IEC 27005가 허용하는 합리적인 분석 방식에 해당하며, 방송시설의 운영 특성과 드론 위협의 특수성을 반영한 위험 식별과 비교 분석에 적합한 방법론으로 판단된다.

나. 위험 수준 산정 체계

위험 수준은 결과와 발생 가능성의 결합으로 정의된다. 본 연구에서는 KS X ISO/IEC 27005의 절차에 따라 영향도 평가와 발생 가능성 평가를 각각 독립적으로 수행한 후, 두 항목의 값을 조합하여 위험 수준을 산정한다. 위험 수준을 산정하는 방법은 [그림 3-3]과 같다.

〔그림 3-3〕 본 연구의 위험 분석(Risk Analysis) 방법



자료: KS X ISO/IEC 27005를 본 연구에 적용하여 재구성

위험 수준(Risk Level)은 결과의 영향도(Impact)와 발생 가능성(Likelihood)을 각각 독립

적으로 분석한 후, 두 요소를 조합하여 단일 위험 수준을 도출하는 구조로 이루어진다. 이는 위험의 크기를 명확히 표현하고 다양한 유형의 위험 간 상대적 비교를 가능하게 하기 위한 표준적 접근 방식이다.

영향도 분석은 특정 위협이 현실화되었을 때 방송시설에 미칠 영향의 정도를 판단하는 절차로, 방송 중단, 설비 손상, 전파 혼신, 안전사고 등 조직의 핵심 기능과 직결되는 요소를 기준으로 이루어진다. 발생 가능성 분석은 식별된 위협이 실제 환경에서 발생할 수 있는 가능성을 판단하는 과정으로, 드론 접근 용이성, 장비 성능 한계, 기존 통제의 실효성, 기술적·운영적 환경 등을 종합적으로 고려하여 수행한다.

마지막으로 위험 수준 산정은 앞서 평가된 두 요소를 조합하여 개별 위험의 등급을 결정하는 단계이다. 본 연구에서는 위협 시나리오에 대한 영향도와 발생 가능성의 조합을 통해 개별적 위험 수준을 산정하며, 이를 통해 위험을 체계적으로 비교하고 우선순위를 설정할 수 있도록 하였다. 산출된 위험 수준은 이후 위험 평가 단계에서 관리 필요성을 판단하는 기준으로 사용된다.

2. 영향도 분석

가. 영향도 분석 방법

영향도 분석은 위협 시나리오가 발생할 경우 방송시설 운영에 미치는 결과의 크기를 정량화하는 절차로, 본 연구에서는 영향도를 서비스 연속성 관점과 안전 관점의 두 축으로 구분하여 평가한다. 즉, 각 위협 시나리오에 대해 방송서비스가 어느 수준까지 저하되거나 중단될 수 있는지, 그리고 인명 및 현장 안전에 어느 수준의 위험이 발생할 수 있는지를 각각 점수화한다. 본 연구의 영향도 점수는 부록에서 제시한 <표 6—1>, <표 6—2>, <표 6—3> 영향도 산정 기준과 영향도 산정식에 근거하여 다음의 절차로 산정한다.

○ 영향도 산정 절차

- 위협 시나리오 발생 시 결과를 ‘서비스 연속성 영향’과 ‘안전 영향’으로 구분하여 해석
- 각 결과를 영향도 산정식에 대응시켜 점수를 부여

본 연구에서는 산정 방식의 이해를 돕기 위해, 대표적인 3개 위협 시나리오를 선정하여 산정 기준을 실제로 적용하는 예시를 제시한다. 다만 본 예시는 영향도 산정 방법을 설명하기 위한 것으로, 전체 자산·전체 위협 시나리오에 대한 영향도 점수의 종합 결과는 위험 수준 산정 단계에서 발생 가능성과 결합하여 일괄적으로 제시한다.

나. 영향도 분석의 예시

서로 성격이 상이한 대표 시나리오 3개를 선정하여, 영향도 점수가 어떻게 도출되었는지를 구체적으로 설명함으로써 분석 결과의 타당성을 보완하고자 한다.

1) 시나리오 사례 1, S-A01-01 (연주소 주조정실 자폭 공격)

○ 시나리오 설명

드론이 연주소 주조정실 인근에서 자폭하거나 폭탄을 투하하여 구조적 손상을 유발

○ 영향도 산정

[서비스 중단 영향(DoS)] : 5점

- 수 시간 ~ 수 일 이상 중단 또는 정상화 불가

[안전 영향] : 5.0점 = (10점 + 5점)/3

[인프라 영향] : 10점, 주조정실 구조적 또는 전면적 파괴

[인명 피해 영향] : 5점, 인명 피해 발생 가능성 매우 높음

[종합 영향도 점수] : 10.0점

- 종합 영향도(10.0) = 서비스 중단(5) + 안전 영향(5.0)

주조정실은 방송 편성·송출을 통합 제어하는 핵심 공간으로, 기능 상실 시 즉각적인 방송 중단이 발생한다. 폭발로 인해 구조적 손상이 발생할 경우 단기간 내 복구가 곤란하며, 송출 제어 기능의 정상화가 장시간 지연될 가능성이 높다. 또한 폭발·파편·화재로 인한 인명 피해 가능성이 매우 크다.

2) 시나리오 사례 2, S-A03-07 (연주소 송신 시설 안테나 충돌)

○ 시나리오 설명

드론이 연주소 송신 시설의 철탑 또는 송신 안테나에 충돌하여 안테나 방향성 또는 구

조물 일부가 손상되는 상황

○ 영향도 산정

송신 안테나는 출력 방향성과 커버리지를 유지하는 핵심 설비로, 물리적 손상 시 특정 지역에서 방송 품질 저하 또는 송출 장애가 발생할 수 있다. 다만 설비 전체가 붕괴되지 않는 경우 즉각적인 전면 중단으로 이어지지는 않을 수 있다.

[서비스 중단 영향(DoS)] : 4점

- 1시간 이상~수 시간 서비스 영향, 권역 단위 장애 가능

[안전 영향] : 3.0점 = (7점 + 2점) / 3

[인프라 영향] : 7점, 주요 송신 인프라 일부 손상

[인명 피해 영향] : 2점, 고소 구조물 손상 또는 드론 추락으로 인한 사고 발생

[종합 영향도 점수] : 7.0점

- 종합 영향도(7.0) = 서비스 중단 영향(4) + 안전 영향(3.0)

3) 시나리오 사례 3, S-A16-08 (방송 고정 중계 링크 전파 간섭)

○ 시나리오 설명

드론 또는 안티드론 재밍으로 인해 STL/TTL 마이크로웨이브 중계 링크에 전파 간섭이 발생하여 방송 신호 전송이 불안정해지는 상황

○ 영향도 산정

전파 간섭은 물리적 설비 손상을 수반하지 않으며 인프라 파괴로 직접 연결되지는 않는다. 다만 중계 링크 품질 저하 또는 단절로 인해 지역 단위 방송 장애가 발생할 수 있다.

[서비스 중단 영향(DoS)] : 4점

- 권역 단위 송출 장애 가능

[안전 영향] : 0.7점 = (1점 + 1점) / 3

[인프라 영향] : 1점, 물리적 설비 손상 없음

[인명 피해 영향] : 1점, 인명 안전 영향 없음

[종합 영향도 점수] : 4.7점

- 종합 영향도(4.7) = 서비스 중단 영향(4) + 안전 영향(0.7)

다. 영향도 분석 결과

앞선 예시와 같은 분석을 모든 시나리오에 분석한 결과는 <표 3-16>과 같다. 자폭·폭발·화재와 같이 시설의 구조적 손상 또는 인명 피해를 유발하는 시나리오는 대부분 높은 영향도로 평가되었으며, 방송송출의 즉각적인 중단 또는 장시간 장애로 이어질 수 있는 것으로 분석되었다.

〈표 3-16〉 위협 시나리오에 대한 영향도 산정표

시나리오 ID	시나리오 설명	서비스 중단	인프라 파괴	인명 피해 영향도	최종 영향도
S-A01-01	자폭·폭탄 투하로 주조정실 구조 손상	5	10	5	10.0
S-A01-02	화염병 등의 위협물 투하로 주조정실 화재 발생	4	8	4	8.0
S-A01-03	장착된 총기로 주조정실 인명 피해 발생	5	1	5	7.0
S-A01-04	불법 정찰로 주조정실 위치·구조 노출	1	3	1	2.3
S-A01-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송출 제어 시스템 침해	3	4	1	4.7
S-A01-06	주조정실 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A01-07	주조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	1	2	1	2.0
S-A02-01	자폭·폭탄 투하로 부조정실 구조 손상	5	9	5	9.7
S-A02-02	화염병 등의 위협물 투하로 부조정실 화재 발생	4	7	4	7.7
S-A02-03	장착된 총기로 부조정실 인명 피해 발생	5	1	5	7.0
S-A02-04	불법 정찰로 부조정실 위치·구조 노출	1	3	1	2.3
S-A02-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 방송 제작 및 제어 시스템 침해	3	4	1	4.7
S-A02-06	부조정실 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A02-07	부조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	1	2	1	2.0
S-A03-01	자폭·폭탄 투하로 연주소 송신 시설 파괴	5	10	5	10.0
S-A03-02	화염병 등의 위협물 투하로 연주소 송신	5	8	4	9.0

	설비 화재 발생				
S-A03-03	장착된 총기로 연주소 송신 설비 인근의 인명 피해 발생	1	1	5	3.0
S-A03-04	불법 정찰로 연주소 송신 설비 위치·구조 노출	1	3	1	2.3
S-A03-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	4	4	1	5.7
S-A03-06	연주소 송신 시설 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A03-07	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	4	7	2	7.0
S-A03-10	요격 잔해가 연주소 송신 시설에 2차 피해	2	3	4	4.3
S-A03-11	요격 후 폭발물이 연주소 송신 시설에 2차 피해	5	10	5	10.0
S-A04-01	자폭·폭탄 투하로 연주소 주변 시설 파괴	1	1	5	3.0
S-A04-02	화염병 등의 위협물 투하로 연주소 주변 시설 화재 발생	1	1	4	2.7
S-A04-03	장착된 총기로 연주소 주변 시설 인근의 인명 피해 발생	1	1	5	3.0
S-A04-04	불법 정찰로 연주소 주변 시설 위치·구조 노출	1	1	1	1.7
S-A04-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 주변 시설 민간 네트워크 사이버 침해	1	1	1	1.7
S-A04-06	연주소 주변 시설 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A04-07	연주소 주변 시설 인근 공역 비행, 시설 충돌로 부수적 피해	1	1	2	2.0
S-A04-10	요격 잔해가 연주소 주변 시설에 2차 피해	1	1	4	2.7
S-A04-11	요격 후 폭발물이 연주소 주변 시설에 2차 피해	1	1	5	3.0
S-A05-01	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	5	10	5	10.0
S-A05-02	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	4	8	4	8.0
S-A05-03	장착된 총기로 송·중계소 수신 설비 인근의 인명 피해 발생	1	1	5	6.0
S-A05-04	불법 정찰로 송·중계소 수신 설비	1	4	1	3.7

	위치·구조 노출				
S-A05-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 수신 시스템 침해	3	4	1	3.7
S-A05-06	송·중계소 수신 시설 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A05-07	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	4	7	2	7.0
S-A05-10	요격 잔해가 송·중계소 수신 시설에 2차 피해	1	3	4	3.3
S-A05-11	요격 후 폭발물이 송·중계소 수신 시설에 2차 피해	5	10	5	10.0
S-A06-01	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	5	10	5	10.0
S-A06-02	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	4	9	4	8.3
S-A06-03	장착된 총기로 송·중계소 송신 설비 인근의 인명 피해 발생	1	1	5	3.0
S-A06-04	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	1	4	1	3.7
S-A06-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	3	4	1	3.7
S-A06-06	송·중계소 송신 시설 인근 공역 단순 침범으로 업무 혼선	1	1	1	1.7
S-A06-07	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	5	7	2	8.0
S-A06-10	요격 잔해가 송·중계소 송신 시설에 2차 피해	1	3	4	3.3
S-A06-11	요격 후 폭발물이 송·중계소 송신 시설에 2차 피해	5	10	5	10.0
S-A07-08	AM 방송 전파 간섭	2	1	1	2.7
S-A08-08	국제 단파 방송 전파 간섭	2	1	1	2.7
S-A09-08	FM 방송 전파 간섭	2	1	1	2.7
S-A10-08	DMB 방송 전파 간섭	2	1	1	2.7
S-A11-08	디지털 TV 방송 전파 간섭	2	1	1	2.7
S-A12-08	UHD 방송 전파 간섭	2	1	1	2.7
S-A13-08	운용 및 제어 신호 전파 간섭	3	1	1	3.7
S-A14-08	프로그램 중계 링크 전파 간섭	4	1	1	4.7
S-A15-08	TV 이동 중계 링크 전파 간섭	4	1	1	4.7
S-A16-08	방송 고정 중계 링크 전파 간섭	4	1	1	4.7

반면, 단순 공역 침범이나 불법 정찰과 같은 시나리오는 직접적인 물리 피해는 제한적이나, 운영 혼선이나 후속 공격 가능성을 증가시키는 요소로 작용하는 것으로 나타났다.

전파 간섭과 같이 방송서비스 품질에 영향을 미치는 시나리오는 송출 불능보다는 품질 저하 중심의 영향으로 평가되었으며, 이후 위험 평가 단계에서는 이러한 영향도 결과를 기준으로 발생 가능성과 결합하여 위험 수준을 산정한다.

3. 발생 가능성 분석

가. 발생 가능성 분석 방법

발생 가능성 분석은 위협 시나리오가 방송시설 환경에서 실제로 현실화될 수 있는 정도를 정량화하는 절차로, 본 연구에서는 방어체계의 구성 수준을 기준으로 발생 가능성을 평가한다. 즉, 동일한 위협 시나리오라 하더라도 방송시설에 적용된 탐지・식별・대응체계의 구축 상태에 따라 실제 사고로 이어질 가능성이 달라진다는 점을 전제로, 발생 가능성을 '특정 방어체계 하에서의 현실화 가능성 수준'으로 정의한다. 본 연구의 발생 가능성 점수는 부록의 <표 6-4>, <표 6-5>, <표 6-6>, <표 6-7>, <표 6-8>, <표 6-9>, <표 6-10> 산정 기준과 발생 가능성 산정식에 근거하여 다음의 절차로 산정한다.

○ 발생 가능성 산정 절차

- 방송시설에 적용된 방어체계의 구성 유형을 기준으로 평가 대상 환경 구분
- 각 방어체계 유형별로 동일한 위협 시나리오가 현실화될 가능성을 해석
- 해석 결과를 발생 가능성 산정식에 대응시켜 점수 부여

산정 방식의 이해를 돕기 위해, 영향도 분석 단계에서 선정한 대표 위협 시나리오를 대상으로 방어체계 유형별 발생 가능성 산정의 적용 예시를 제시한다. 다만 본 예시는 발생 가능성 산정 방법을 설명하기 위한 것으로, 전체 자산・전체 위협 시나리오에 대한 발생 가능성 점수의 종합 결과는 위험 수준 산정 단계에서 영향도와 결합하여 일괄적으로 제시한다.

나. 방어체계 예시 유형 정의

방어체계 수준에 따른 발생 가능성 분석을 수행하기 위하여, 방송시설에서 현실적으로 적용 가능한 드론 방어체계 운용 유형을 설정하였다. 여기서 제시하는 운용 유형은 특정 시설의 실제 구축 현황을 단정적으로 나타내는 것이 아니라, 방어체계 구성 수준에 따라 발생 가능성이 어떻게 달라질 수 있는지를 설명하기 위한 예시적 유형이다. 운용 유형에 따른 방어 수준은 부록의 <표 6-5>을 기준으로 산정하고, 각 유형은 다음과 같다.

1) 운용 유형 1 : 감시·경비 중심 운용 유형

○ 주요 운용 장비

- CCTV(고정형·회전형)
- 일반 영상 관제 시스템
- 출입 통제 및 인력 경비

○ 운용 특성

- 드론을 전제로 한 전용 탐지·식별 기능 없음
- 위협 인지는 육안 관찰 또는 사후 확인에 의존
- 능동적 대응 및 통제 불가

○ 대표적 예시 유형 설정의 이유

드론 위협을 전제로 한 탐지·대응체계가 구축되지 않은 일반적인 시설 보안 수준을 대표하는 유형으로, 드론 대응 계 부재 상태로 기준선을 설정하기 위함이다.

○ 방어 수준, 1점

공역을 대상으로 하는 CCTV가 없기 때문에 무방비 상태와 같아 1점 부여.

2) 운용 유형 2 : RF 스캐너 중심의 드론 탐지 장비 중심 운용 유형

○ 주요 운용 장비

- 드론 RF 스캐너

○ 운용 특성

- 드론 접근 여부 탐지 가능
- 경보 발령 및 상황 인지 중심 대응
- 즉각적 차단·통제는 곤란

○ 대표적 예시 유형 설정의 이유

전파 방사를 수반하지 않는 수동적 탐지 방식만으로 드론 위협을 인지하는 운용 환경을 대표하는 유형으로, 탐지 기능 확보 이후 대응 수단이 유관 기관 연계로 진행할 경우를 분석하기 위함이다.

○ 방어 수준, 3점

RF를 이용한 탐지는 드론의 항법 방식에 따라서 탐지 가능성이 낮아지기 때문에 3점 부여.

3) 운용 유형 3 : RF 기반 다층 탐지와 전방위 소프트킬 장비 운용 유형

○ 주요 운용 장비

- RF 탐지 센서
- 드론 식별용 영상 센서
- RF/GNSS 재밍 장비

○ 운용 특성

- 탐지 이후 무력화 가능
- 위협 드론의 비행 제한 또는 이탈 유도
- 전파 혼신 등 운용 부작용 가능성 존재

○ 대표적 예시 유형 설정의 이유

탐지 이후 무력화가 가능하나, 전방위 전파 방사로 인한 혼신 및 부작용 가능성이 동시에 존재하는 경우를 분석하기 위함이다.

○ 방어 수준, 5점

소프트킬의 간단한 형태로 사정거리가 짧아 즉각 대응이 어렵다는 점에서 5점 부여.

○ 전파 간섭 가능성, 6.4점

전파 간섭 가능성은 부록의 <표 6-6>과 <표 6-7>과 산정식에 의해서 산정되며, 장비마다 산정 결과가 다르지만, 대표적인 재머 장비를 기준으로 산정하였다.

[주파수 정합도] : 10점

- 드론 통신 채널 식별 없이 해당 주파수 대역 전체를 포괄 송출하는 구조

[시간 정합도] : 3점

- 무력화 시 송출하는 형태

[불요파 억제력] : 1점

- 시중에 도입할 수 있는 인증된 재머 기준, 불요파 억제력 우수

[전파 방사 각도] : 10점

- 드론 방향과 무관한 전방위(360°) 출력 기준

[전력 세기] : 8점

- 고출력 기반 송출로 인접 수신 설비에 포화·블로킹 영향 우려

[전파 간섭 가능성] : 6.4점 = {2*(10 + 3) + 1 + 10 + 8 } / 7

4) 운용 유형 4 : RF 기반 다층 탐지와 정밀 소프트킬 장비 운용 유형

○ 주요 운용 장비

- RF 탐지 센서
- 드론 식별용 영상 센서
- RF/GNSS 스마트 재밍, 정밀 통제 가능 장비

○ 운용 특성

- 탐지 이후 즉각적인 대응 가능
- 위협 드론의 비행 제한 또는 이탈 유도
- 전파 혼신 등 운용 부작용이 존재하지 않음

○ 대표적 예시 유형 설정의 이유

전파 방사를 수반하되, 전파 간섭을 최소화한 경우의 운용 효과를 분석하기 위한 유형으로, 소프트킬 운용 종류에 따른 기술적 장단점을 비교하기 위함이다.

○ 방어 수준, 6점

소프트킬 사용 형태 중 긴 사정거리로 대응이 가능하지만, 낮은 군집 드론 대응 능력, 항법 의존도로 인하여 6점 부여.

○ 전파 간섭 가능성, 2.6점

전파 간섭 가능성은 부록의 <표 6-6>과 <표 6-7>과 산정식에 의해서 산정되며, 장비마다 산정 결과가 다르지만, 대표적인 정밀 소프트킬 장비를 기준으로 산정하였다.

[주파수 정합도] : 1점

- 드론의 통신 채널을 식별하여 필요한 주파수와 시간에만 선택 송출하는 구조

[시간 정합도] : 1점

- 탐지·식별 이후 무력화가 필요한 시점에만 단시간 송출하는 운용 방식

[불요파 억제력] : 1점

- 인증된 정밀 소프트킬 장비 기준, 불요파 억제력 우수

[전파 방사 각도] : 10점

- 드론 방향과 무관한 전방위 출력 기준

[전력 세기] : 3점

- 고출력 기반 송출로 인접 수신 설비에 포화·블로킹 영향 우려

[전파 간섭 가능성] : 2.6점 = {2*(1 + 1) + 1 + 10 + 3 } / 7

5) 운용 유형 5 : RF 기반 다층 탐지 탐지와 단일 하드킬 장비(레이저) 운용 유형

○ 주요 운용 장비

- RF 탐지 센서
- 드론 식별용 영상 센서
- 레이저 요격 장비

○ 운용 특성

- 탐지 이후 즉각적인 대응 가능
- 요격 통제 수준 제한적
- 잔해 추락 위험 존재

○ 대표적 예시 유형 설정의 이유

하드킬 기반 대응의 효과와 안전성 한계를 함께 평가하기 위함이다.

○ 방어 수준, 7점

하드킬을 사용한 부분 대응 형태 중 요격 잔해가 떨어지는 부작용이 존재 하지만. 소프트킬보다 긴 사거리로 군집 드론까지 즉각 대응이 가능하다는 점에서 7점 부여.

○ 요격 통제 가능성, 5점

요격 통제 가능성은 부록의 <표 6-10>에 의해서 산정되며, 탐지 장비와 무력화 장비의 결합에 따라 산정 결과가 다르지만, 대표적인 레이저 요격 장비를 기준으로 산정하였다.

[요격 통제 가능성] : 5점

- RF 탐지·영상 식별 기반으로 요격 타이밍 또는 지점에 대한 제한적 조정은 가능하나, 레이저 요격 특성상 잔해 낙하 범위 통제는 부분적으로 가능

6) 운용 유형 6 : 레이다 중심의 다층 탐지 장비와 단일 하드킬 장비 운영

○ 주요 운용 장비

- 드론 탐지 레이다
- 드론 식별용 영상 센서
- 레이저 요격 장비

○ 운용 특성

- 드론 항법 방식에 관계 없이 탐지 가능
- 즉각적 차단·통제 가능
- 탐지 시 레이다 운용 대역에 대한 전파 방사 존재

○ 대표적 예시 유형 설정의 이유

드론의 항법 방식과 무관하게 탐지·대응이 가능한 레이다 기반 다층 탐지와 하드킬을 결합한 고수준 방어 환경을 대표하여, 높은 대응력을 갖춘 운용 유형을 평가하기 위함.

○ 방어 수준, 8점

요격 통제가 원활하고 드론의 항법 방식에 의존하지 않고 탐지한다는 점에서 8점 부여.

○ 전파 간섭 가능성, 8.1점

전파 간섭 가능성은 부록의 <표 6-6>과 <표 6-7>과 산정식에 의해서 산정되며, 장비마다 산정 결과가 다르지만, 대표적인 레이다 드론 탐지 장비를 기준으로 산정하였다.

[주파수 정합도] : 9점

- 드론 탐지를 위해 대역 전체를 포괄 송출하는 구조

[시간 정합도] : 10점

- 탐지 여부와 무관하게 상시 또는 장시간 지속 송출되는 운용 방식

[불요파 억제력] : 1점

- 시중에 도입할 수 있는 인증된 레이다 기준, 불요파 억제력 우수

[전파 방사 각도] : 10점

- 회전 또는 전자식 스캔 방식으로 전방위(360°)에 전파가 방사됨

[전력 세기] : 8점

- 고출력 기반 송출로 인접 수신 설비에 포화·블로킹 영향 우려

[전파 간섭 가능성] : 8.1점 = {2*(9 + 10) + 1 + 10 + 8 } / 7

○ 요격 통제 가능성, 8점

요격 통제 가능성은 부록의 <표 6-10>에 의해서 산정되며, 탐지 장비와 무력화 장비의 결합에 따라 산정 결과가 다르지만, 대표적인 레이저 요격 장비를 기준으로 산정하였다.

[요격 통제 가능성] : 8점

- 레이다 탐지로 표적의 위치·진입을 정밀하게 추적할 수 있는 이유로, 요격 타이밍·지점 선택이 가능하며 낙하 위험 구역을 회피하는 수준의 운용이 가능한 상태이다.

나. 발생 가능성 분석 예시

본 연구에서는 발생 가능성을 위협 시나리오 자체의 고정된 속성이 아닌, 방송시설에 적용되는 방어체계의 운용 유형에 따라 달라지는 값으로 평가한다. 즉, 동일한 위협 시나리오라 하더라도 탐지・대응・통제 수준에 따라 실제 현실화 가능성은 서로 다르게 나타날 수 있다.

따라서 방송시설 환경에서 대표성이 높은 위협 시나리오 3개를 선정하여, 방어체계 유형별로 발생 가능성이 어떻게 변화하는지를 예시적으로 제시한다. 이 과정은 발생 가능성 산정 결과를 단순 비교하는 데 그치지 않고, 방어 수준, 전파 간섭 가능성, 요격 통제 가능성 등 복수의 변수가 발생 가능성에 어떤 구조로 작용하는지를 단계적으로 해석하기 위한 가이드라인의 성격을 가진다.

이를 통해 방어체계 운용 방식의 차이가 위험 수준 형성에 미치는 영향을 비교・검증하고, 본 연구의 발생 가능성 산정 구조가 방송시설 환경의 특성을 합리적으로 반영하고 있음을 확인하고자 한다. 전체 시나리오에 대한 발생 가능성 산정 결과는 이후 위험 수준 산정 단계에서 일괄적으로 제시한다.

1) 시나리오 사례 1, S-A01-01 (연주소 주조정실 자폭 공격)

○ 시나리오 설명

드론이 연주소 주조정실 인근에서 자폭하거나 폭탄을 투하하여 구조적 손상을 유발하는 상황이다.

○ 발생 가능성 산정

본 시나리오는 주조정실이라는 고보안・내부 핵심 공간을 표적으로 하므로, 드론이 외부에서 침투하여 자폭 공격을 수행하기까지 요구되는 기술적・물리적 진입장벽이 매우 높다. 이에 따라 해당 시나리오의 전반적인 발생 가능성은 방송시설 환경에서 구조적으로 낮은 수준으로 평가된다.

[기술적 수행 용이성] : 2점

- 내부 비행 후 자폭은 특수 조직급 훈련 수준 요구에 해당함

[공격 자산 획득성] : 3점

- 폭발물은 고난도 확보 수단 요구에 해당함

[표적 정보 노출도] : 7점

- 주조정실 위치 및 동선은 제한적 정보 접근 필요에 해당함

[물리적 접근성] : 3점

- 외부에서 내부 공간까지의 침투는 접근 난이도 매우 높음에 해당함

[공격 실행 가능성] : 3.75점 = (2 + 3 + 7 + 3) / 4

[유형별 드론 위협 발생 가능성]

- 유형 1, 드론 위협 발생 가능성 : 3.8점
- 유형 2, 드론 위협 발생 가능성 : 2.4점
- 유형 3, 드론 위협 발생 가능성 : 1.4점
- 유형 4, 드론 위협 발생 가능성 : 0.9점
- 유형 5, 드론 위협 발생 가능성 : 0.6점
- 유형 6, 드론 위협 발생 가능성 : 0.3점

2) 시나리오 사례 2, S-A14-08 (프로그램 중계 링크 전파 간섭)

○ 시나리오 설명

STL에서 사용되는 프로그램 중계 링크 1.7GHz 대역에 대한 전파 간섭이 발생하는 상황이다.

○ 발생 가능성 산정

전파 확산 특성상 방어체계의 전파 방사 방식과 운용 형태에 따라 간섭 발생 가능성의 존재 여부와 그 편차가 발생하는 유형에 해당한다. 이에 따라 전파 간섭이 발생하는 유형 3, 4, 6에 대하여 발생 가능성을 산정한다.

[전파 간섭 특성] : 2점

- 1.7GHz 대역은 전파 확산, 직진 특성 혼재, 부록의 <표 6-8>에 의해 산정

[유형별 전파 간섭 가능성], 방어체계 유형 사전 정의

- 유형 3, 전파 간섭 발생 가능성 : 6.4점
- 유형 4, 전파 간섭 발생 가능성 : 2.6점
- 유형 6, 전파 간섭 발생 가능성 : 8.1점

[유형별 발생 가능성]

- 유형 3, 드론 위협 발생 가능성 : 4.3점
- 유형 4, 드론 위협 발생 가능성 : 1.7점
- 유형 6, 드론 위협 발생 가능성 : 5.4점

3) 시나리오 사례 3, S-A06-10 (송·중계소 송신 시설의 요격 잔해에 의한 2차 피해)

○ 시나리오 설명

요격 후 추락 잔해로 인한 송·중계소 송신 시설에 2차 피해가 발생하는 상황이다.

○ 발생 가능성 산정

탐지 성능 차이로 요격 통제 가능성이 다른 유형 5, 6에 대해 발생 가능성을 산정한다.

[인적 노출도] : 2점

- 비상주 인원만 간헐적으로 출입하는 외부 설비로, 상시 인명 피해 가능성 낮음

[시설 노출도] : 10점

- 송신 핵심 설비가 외부에 직접 노출되어 잔해 낙하 시 송신 기능 상실 가능

[유형별 요격 통제 가능성], 방어체계 유형 사전 정의

- 유형 5, 요격 통제 가능성 : 5점
- 유형 6, 요격 통제 가능성 : 8점

[유형별 발생 가능성]

- 유형 5, 드론 위협 발생 가능성 : 2.2점
- 유형 6, 드론 위협 발생 가능성 : 0.5점

다. 발생 가능성 결과

1) 드론 위협 시나리오의 발생 가능성

드론 위협 시나리오에 대한 발생 가능성 분석 결과는 <표 3-17>과 같다. 본 표는 각 위협 시나리오에 대해 기술적 난이도, 공격 자산 획득성, 표적 정보 노출도, 물리적 접근성을 종합하여 방어체계 유형별 발생 가능성을 산정한 결과를 제시한다.

〈표 3-17〉 위협 시나리오에 대한 발생 가능성 산정표

시나리오 ID	시나리오 설명	기술적 난이도	공격 자산 획득성	표적 정보 노출도	물리적 접근성	유형별 발생 가능성					
						유형 1	유형 2	유형 3	유형 4	유형 5	유형 6
S-A01-01	자폭·폭탄 투하로 주조정실 구조 손상	2	3	7	3	3.8	2.4	1.4	0.9	0.6	0.3
S-A01-02	화염병 등의 위협물 투하로 주조정실 화재 발생	2	7	7	3	4.8	3.0	1.7	1.2	0.8	0.4
S-A01-03	장착된 총기로 주조정실 인명 피해 발생	1	1	7	3	3.0	1.9	1.1	0.8	0.5	0.3
S-A01-04	불법 정찰로 주조정실 위치·구조 노출	3	10	7	3	5.8	3.7	2.1	1.4	0.9	0.5
S-A01-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송출 제어 시스템 침해	1	3	3	3	2.5	1.6	0.9	0.6	0.4	0.2
S-A01-06	주조정실 인근 공역 단순 침범으로 업무 혼선	10	10	7	10	9.3	5.9	3.3	2.3	1.5	0.8
S-A01-07	주조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	10	10	7	10	9.3	5.9	3.3	2.3	1.5	0.8
S-A02-01	자폭·폭탄 투하로 부조정실 구조 손상	2	3	8	3	4.0	2.6	1.4	1.0	0.6	0.4
S-A02-02	화염병 등의 위협물 투하로 부조정실 화재 발생	2	7	8	3	5.0	3.2	1.8	1.3	0.8	0.5
S-A02-03	장착된 총기로 부조정실 인명 피해 발생	1	1	8	3	3.3	2.1	1.1	0.8	0.5	0.3

S-A02-04	불법 정찰로 부조정실 위치·구조 노출	3	10	8	3	6.0	3.8	2.0	1.5	0.9	0.6
S-A02-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 방송 제작 및 제어 시스템 침해	1	3	3	3	2.5	1.6	0.8	0.6	0.4	0.3
S-A02-06	부조정실 인근 공역 단순 침범으로 업무 혼선	10	10	8	10	9.5	6.1	3.4	2.4	1.5	0.9
S-A02-07	부조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	10	10	8	10	9.5	6.1	3.4	2.4	1.6	0.9
S-A03-01	자폭·폭탄 투하로 연주소 송신 시설 파괴	4	3	9	10	6.5	4.2	2.3	1.6	1.0	0.6
S-A03-02	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	5	7	8	10	7.5	4.8	2.7	1.9	1.2	0.7
S-A03-03	장착된 총기로 연주소 송신 설비 인근의 인명 피해 발생	1	1	3	10	3.8	2.4	1.4	0.9	0.6	0.3
S-A03-04	불법 정찰로 연주소 송신 설비 위치·구조 노출	8	10	9	10	9.3	5.9	3.3	2.3	1.5	0.8
S-A03-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	1	3	3	10	4.3	2.7	1.5	1.1	0.7	0.4
S-A03-06	연주소 송신 시설 인근 공역 단순 침범으로 업무 혼선	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A03-07	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A04-01	자폭·폭탄 투하로 연주소 주변 시설 파괴	4	3	10	10	6.8	4.3	2.4	1.7	1.1	0.6
S-A04-02	화염병 등의 위협물 투하로 연주소 주변 시설 화재 발생	5	7	10	10	8.0	5.1	2.9	2.0	1.3	0.7
S-A04-03	장착된 총기로 연주소 주변 시설 인근의 인명 피해 발생	1	1	10	10	5.5	3.5	2.0	1.4	0.9	0.5
S-A04-04	불법 정찰로 연주소 주변 시설 위치·구조 노출	9	10	10	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A04-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 주변 시설 민간 네트워크 사이버 침해	3	5	6	10	6.0	3.8	2.2	1.5	1.0	0.5
S-A04-06	연주소 주변 시설 인근 공역 단순 침범으로 업무 혼선	10	10	10	10	10.0	6.4	3.6	2.5	1.6	0.9
S-A04-07	연주소 주변 시설 인근 공역 비행, 시설 충돌로 부수적 피해	10	10	10	10	10.0	6.4	3.6	2.5	1.6	0.9

S-A05-01	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	4	3	9	10	6.5	4.2	2.3	1.6	1.0	0.6
S-A05-02	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	5	7	8	10	7.5	4.8	2.7	1.9	1.2	0.7
S-A05-03	장착된 총기로 송·중계소 수신 설비 인근의 인명 피해 발생	1	1	3	10	3.8	2.4	1.4	0.9	0.6	0.3
S-A05-04	불법 정찰로 송·중계소 수신 설비 위치·구조 노출	8	10	9	10	9.3	5.9	3.3	2.3	1.5	0.8
S-A05-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 수신 시스템 침해	1	3	3	10	4.3	2.7	1.5	1.1	0.7	0.4
S-A05-06	송·중계소 수신 시설 인근 공역 단순 침범으로 업무 혼선	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A05-07	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A06-01	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	4	3	9	10	6.5	4.2	2.3	1.6	1.0	0.6
S-A06-02	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	5	7	8	10	7.5	4.8	2.7	1.9	1.2	0.7
S-A06-03	장착된 총기로 송·중계소 송신 설비 인근의 인명 피해 발생	1	1	3	10	3.8	2.4	1.4	0.9	0.6	0.3
S-A06-04	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	8	10	9	10	9.3	5.9	3.3	2.3	1.5	0.8
S-A06-05	자체적인 또는 투하한 전자기기를 통한 사이버 공격으로 송신 시스템 침해	1	3	3	10	4.3	2.7	1.5	1.1	0.7	0.4
S-A06-06	송·중계소 송신 시설 인근 공역 단순 침범으로 업무 혼선	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9
S-A06-07	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	10	10	9	10	9.8	6.2	3.5	2.4	1.6	0.9

드론 위협 시나리오에 대한 발생 가능성 분석 결과, 단순 공역 침범, 불법 정찰, 비의도적 충돌과 같이 기술적 난이도가 낮고 물리적 접근이 용이한 시나리오는 전반적으로 높은 발생 가능성을 보이는 것으로 나타났다. 반면 자폭·폭발, 무장 공격, 정밀한 사이버 침해와 같이 사전 준비와 자산 확보가 요구되는 시나리오는 상대적으로 낮은 발생 가능성으로 평가되었다.

2) 안티드론 위협 시나리오의 발생 가능성

안티드론 위협 시나리오로 인해 발생할 수 있는 위협은 적용되는 대응 방식의 특성에 따라 전파 간섭 가능성과 하드킬에 의한 2차 피해 발생 가능성의 두 범주로 나누어 산정하였다.

① 전파 방사로 인한 전파 간섭 발생 가능성

전파 방사로 인한 전파 간섭 발생 가능성 분석 결과는 <표 3-18>과 같다. 본 표는 방송 주파수, 중계 링크 및 제어 신호를 대상으로, 전파 방사를 수반하는 안티드론 운용 유형별 전파 간섭 발생 가능성을 비교·산정한 결과를 제시한다.

〈표 3-18〉 전파 방사로 인한 전파 간섭 발생 가능성 산정표

시나리오 ID	시나리오 설명	전파 간섭 특성	유형별 전파 간섭 가능성			유형별 발생 가능성		
			유형 3	유형 4	유형 6	유형 3	유형 4	유형 6
S-A07-08	AM 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A08-08	국제 단파 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A09-08	FM 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A10-08	DMB 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A11-08	디지털 TV 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A12-08	UHD 방송 전파 간섭	3	6.4	2.6	8.1	6.4	2.6	8.1
S-A13-08	운용 및 제어 신호 전파 간섭	2	6.4	2.6	8.1	4.3	1.7	5.4
S-A14-08	프로그램 중계 링크 전파 간섭	2	6.4	2.6	8.1	4.3	1.7	5.4
S-A15-08	TV 이동 중계 링크 전파 간섭	2	6.4	2.6	8.1	4.3	1.7	5.4
S-A16-08	방송 고정 중계 링크 전파 간섭	1	6.4	2.6	8.1	2.1	0.9	2.7

전파 방사로 인한 전파 간섭 발생 가능성 분석 결과, 전파 방사를 수반하는 안티드론 운용 유형에서 방송서비스 및 관련 전송·제어 신호에 대한 간섭 가능성이 나타나는 것으로 분석되었다. 특히 전방위 전파 방사를 사용하는 운용 유형인 유형 3, 6에서는 전반적으로 높은 전파 간섭 가능성이 평가된 반면, 주파수 및 시간 정합도를 적용한 정밀 운용 유형 4에서는 상대적으로 낮은 수준의 발생 가능성이 나타났다.

② 하드킬에 의한 2차 피해 발생 가능성

하드킬 운용에 따른 2차 피해 발생 가능성 분석 결과는 <표 3-19>와 같다. 본 표는 요격 통제 가능성에 따른 잔해 낙하 및 폭발물 확산으로 인한 2차 피해 발생 가능성을 비교·산정한 결과를 제시한다.

〈표 3-19〉 하드킬에 의한 2차 피해 발생 가능성 산정표

시나리오 ID	시나리오 설명	인적노출도	시설노출도	유형별 요격 통제 가능성		유형별 발생 가능성	
				유형 5	유형 6	유형 5	유형 6
S-A03-10	요격 잔해가 연주소 송신 시설에 2차 피해	6	10	5	8	2.9	0.7
S-A03-11	요격 후 폭발물이 연주소 송신 시설에 2차 피해	6	10	5	8	2.9	0.7
S-A04-10	요격 잔해가 연주소 주변 시설에 2차 피해	10	2	5	8	2.2	0.5
S-A04-11	요격 후 폭발물이 연주소 주변 시설에 2차 피해	10	2	5	8	2.2	0.5
S-A05-10	요격 잔해가 송·중계소 수신 시설에 2차 피해	2	10	5	8	2.2	0.5
S-A05-11	요격 후 폭발물이 송·중계소 수신 시설에 2차 피해	2	10	5	8	2.2	0.5
S-A06-10	요격 잔해가 송·중계소 송신 시설에 2차 피해	2	10	5	8	2.2	0.5
S-A06-11	요격 후 폭발물이 송·중계소 송신 시설에 2차 피해	2	10	5	8	2.2	0.5

요격 과정에서 잔해 낙하로 인한 인명 및 시설 피해 가능성은 요격 통제가 가능한 운용 환경에서는 전반적으로 낮은 수준으로 평가되었다. 표적의 위치와 요격 시점을 고려한 통제된 운용이 이루어질 경우, 잔해 낙하로 인한 피해 발생 가능성은 제한적인 범위 내에서 관리 가능한 수준으로 나타났다. 이러한 결과는 하드킬 운용 시 요격 통제 능력이 2차 피해 위험을 완화하는 핵심 요소임을 의미한다.

4. 위험 수준 산정

산정된 영향도와 발생 가능성을 통해 산정한 위험 수준의 결과는 부록의 <표 6-11>이다. 해당 표는 본 연구의 위험 분석, 평가, 대응까지의 과정과 추후 안티드론 구축 방안을 제시할 근거로써 사용되며, 본 연구의 가장 핵심적인 결과이다. 해당 표를 요약하자면, 방송시설에 대한 드론 위협 시나리오는 자산의 중요도와 위협의 성격에 따라 위험 수준이 뚜렷하게 구분되는 양상을 보인다. 특히 자폭·폭탄 투하, 화재 유발, 송·수신 설비 파괴와 같이 방송 기능의 직접적인 상실로 이어지는 시나리오는 대부분의 자산군에서 높은 위험 수준을 나타내며, 방송 연속성에 중대한 영향을 미칠 수 있는 핵심 위협으로 확인되었다.

반면, 불법 정찰이나 단순 공역 침범과 같은 시나리오는 영향도 자체는 상대적으로 낮으나 발생 가능성이 높아, 전반적으로 중간 수준의 위험 수준을 형성하는 경향을 보였다. 이는 즉각적인 물리적 피해보다는 반복적 발생 가능성과 누적 위험 측면에서 관리가 필요한 위협 유형임을 시사한다.

연주소 및 송·중계소 송·수신 시설과 같이 방송 체계의 핵심 기능을 담당하는 자산에서는 동일한 위협 시나리오라도 위험 수준이 상대적으로 높게 산정되었으며, 주변 시설이나 보조 자산에 비해 위험 민감도가 큰 것으로 나타났다. 이는 자산의 기능적 중요도가 위험 수준에 직접적인 영향을 미친다는 점을 보여준다.

또한 전파 간섭이나 요격 잔해 낙하와 같은 안티드론 대응 과정에서 발생하는 위협 시나리오는 적용되는 운용 유형에 따라 위험 수준의 차이가 명확하게 나타났으며, 대응 수단의 특성과 운용 방식이 위험 수준을 좌우하는 주요 요인으로 확인되었다.

이러한 결과는 방송시설 보호를 위한 위험 관리에서 단일 위협의 발생 여부뿐 아니라, 자산의 중요도와 대응 방식에 따른 위험 증폭 가능성을 함께 고려해야 함을 시사한다.

제 5 절 방송시설 위험 평가(Risk Evaluation) 단계

1. 방송시설 위험 평가 개요

본 절에서는 앞 절에서 도출한 자산별・시나리오별 위험 분석 결과를 바탕으로, KS X ISO/IEC 27005의 절차에 따라 방송시설 보호 관점의 위험 평가를 수행한다. 위험 평가는 식별된 위험을 실제 의사결정에 연계하기 위한 단계로, 위험 수준을 기준으로 위험의 허용 여부와 관리 수준을 체계적으로 구분하는 데 목적이 있다.

이를 위해 본 연구에서는 위험 수준별 허용 범위를 정의하고, 수용 가능한 위험과 추가적인 관리・대응이 필요한 위험을 구분한다. 또한 이러한 위험 수준 분류 결과를 토대로 대응 우선순위를 도출하여, 제한된 자원과 제도적 환경 하에서 방송시설에 적합한 안티드론 대응 전략과 보호체계 구축 방향을 합리적으로 설정하고자 한다.

2. 위험 허용 기준 설정

본 연구에서는 앞 절에서 도출한 위험 수준을 실제 의사결정에 활용하기 위해, 위험의 수용 여부와 대응 우선순위를 판단할 수 있는 위험 허용 기준을 설정한다. 위험 허용 기준은 단순한 점수 구분이 아니라, 방송시설의 공공성, 방송 연속성, 인명 안전, 제도・규제 환경 등을 종합적으로 고려하여 위험을 관리 가능한 수준으로 분류하기 위한 판단 기준으로 활용된다.

방송시설은 국가 기간통신 및 공공 정보 전달 기능을 수행하는 핵심 인프라로서, 일반 시설과 동일한 수준의 위험 수용 기준을 적용하기에는 한계가 있다. 특히 인명 피해 가능성, 장시간 방송 중단, 광역 서비스 장애로 이어질 수 있는 위험은 보수적으로 판단할 필요가 있다. 이에 따라 본 연구에서는 위험 점수의 절대값뿐 아니라, 위험이 미치는 영향의 성격을 함께 고려할 수 있도록 단계별 위험 허용 기준을 설정하였다.

본 연구에서 설정한 위험 허용 기준은 <표 3−20>과 같이 다섯 단계(Level A~E)로 구분되며, 각 단계별로 위험 수용 여부와 관리・대응 방향을 명확히 정의하였다.

〈표 3-20〉 위험 허용 기준

구분	위험 수준(R)	위험 허용 여부	관리·대응 방향	색 표시
Level A	R > 60	수용 불가	즉시 위험 저감·회피 조치	
Level B	40 < R ≤60	수용 불가	단기 내 위험 저감·회피 계획 수립 및 이행	
Level C	20 < R ≤40	조건부 수용	우선순위 관리 대상, 단계적 저감 조치	
Level D	10 < R ≤ 20	수용	관리·모니터링 중심 대응	
Level E	R ≤10	수용	현 상태 유지 및 관찰	

Level A는 인명 피해 가능성 또는 방송 연속성의 중대한 훼손과 직접적으로 연계되는 위험으로, 방송시설 보호 관점에서 어떠한 조건에서도 수용이 불가능한 위험으로 분류된다. 해당 수준의 위험은 보호체계 구축 시 최우선적으로 제거 또는 회피되어야 하며, 구조적 회피 또는 강력한 기술적 저감 조치가 요구된다.

Level B는 즉각적인 위험 대응까지는 요구되지 않으나, 현재 상태로의 유지는 허용될 수 없는 위험을 의미한다. 이 단계의 위험은 단기간 내 저감 또는 회피 조치가 반드시 수행되어야 하며, 대응 지연 시 상위 위험(Level A)으로 전이될 가능성을 내포한다. 따라서 보호체계 구축 및 운용 개선 과정에서 우선적인 저감 대상 위험으로 관리된다.

Level C은 추가적인 저감 조치나 운용 절차 개선을 전제로 한 경우에 한해 관리가 가능한 위험을 의미한다. 해당 위험은 무조건적인 수용 대상은 아니며, 대응 수단 보강, 운용 규칙 정비, 감시 체계 강화 등을 통해 위험 수준을 낮추는 것을 전제로 한 우선순위 대응 대상으로 분류된다.

Level D는 일정 수준의 위험은 존재하나, 표준 운영 절차, 상시 모니터링, 교육·훈련 등을 통해 관리가 가능한 위험으로 판단된다. 이 단계의 위험은 비용 대비 효과를 고려한 제한적 보완 조치 또는 관리 중심의 대응이 적절하며, 즉각적인 기술적 개입이 필수적인 수준은 아니다.

Level E는 위험 수준이 낮아 현재의 운용 환경에서 추가적인 대응 없이도 수용 가능한 범위로 판단되는 위험을 의미한다. 해당 위험은 관찰 수준에서 관리되며, 운용 환경 변화, 시설 구조 변경, 위협 환경 변화 시 재평가를 수행하는 방식으로 관리한다.

3. 위험 수준 분류

가. 위험 수준 분류 정의

본 연구에서는 앞 절에서 산정한 위험 수준(R)을 위험 허용 기준(Level A~E)에 적용하여, 각 위협 시나리오의 위험을 분류하였다. 위험 분류는 위험의 상대적 크기와 관리 필요성을 직관적으로 식별하기 위한 단계로, 본 절에서는 위험의 대응 우선순위를 논의하기에 앞서 위험 수준의 구분에 초점을 두었다.

위험 분류 결과는 위험 분석 결과인 부록의 위험 수준 산정표 <표 6—11>에 반영하여, 각 시나리오의 위험 수준이 해당하는 위험 허용 수준에 따라 색상으로 구분 표시하였다. 이를 통해 위험 수준에 따른 분포를 시각적으로 확인할 수 있도록 하였으며, 위험이 집중되는 영역과 상대적으로 낮은 위험 영역을 한눈에 파악할 수 있도록 하였다.

나. 위험 대응 우선 순위 결정

본 연구에서는 위험 수준 분류 결과를 바탕으로 보호체계 구축 및 운용 단계에서 참고할 수 있는 위험 대응 우선순위를 도출하였다. 다만 시설의 운영 환경, 예산, 인력 구성 등 내부 여건에 따라 대응 우선순위는 달라질 수 있으므로, 외부 기관의 관점에서 세부 대응 순서를 단정적으로 제시하는 데에는 한계가 있다.

위험 대응 우선순위는 별도의 안티드론 보호체계가 적용되지 않은 현 방송시설의 기본 방어 수준(운용 유형 1)을 기준으로 산정한 결과로, 보호체계 미구축 상태에서 위협 시나리오 간 상대적 위험도와 대응 필요성을 판단하기 위한 기준선으로 활용된다.

위험 대응 우선순위는 영향도와 발생 가능성을 종합한 위험 수준 산정값을 기준으로 설정하였으며, 위험 수준이 높을수록 대응 필요성이 큰 것으로 판단하였다. 이에 따른 위험 대응 우선순위는 <표 3-21>과 같다.

〈표 3-21〉 위험 대응 우선 순위 - 운용 유형 1 (현행 체계)

위험 허용 기준	시나리오 ID	우선 순위	시나리오 설명	위험 수준
Level A	S-A06-07	1	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	78.4
	S-A03-07	2	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	68.6
	S-A05-07	3	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	68.6
	S-A03-02	4	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	67.5
	S-A03-01	5	자폭·폭탄 투하로 연주소 송신 시설 파괴	65.0
	S-A05-01	6	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	65.0
	S-A06-01	7	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	65.0
	S-A06-02	8	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	62.3
Level B	S-A05-02	9	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	60.0
Level C	S-A02-01	10	자폭·폭탄 투하로 부조정실 구조 손상	38.8
	S-A02-02	11	화염병 등의 위협물 투하로 부조정실 화재 발생	38.5
	S-A01-02	12	화염병 등의 위협물 투하로 주조정실 화재 발생	38.4
	S-A01-01	13	자폭·폭탄 투하로 주조정실 구조 손상	38.0
	S-A05-04	14	불법 정찰로 송·중계소 수신 설비 위치·구조 노출	34.4
	S-A06-04	15	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	34.4
	S-A03-05	16	사이버 공격으로 송신 시스템 침해	24.5
	S-A02-03	17	장착된 총기로 부조정실 인명 피해 발생	23.1
	S-A05-03	18	장착된 총기로 송·중계소 수신 설비 인근의 인명 피해 발생	22.8
	S-A04-02	19	화염병 등의 위협물 투하로 연주소 주변 시설 화재 발생	21.6
	S-A03-04	20	불법 정찰로 연주소 송신 설비 위치·구조 노출	21.4
	S-A01-03	21	장착된 총기로 주조정실 인명 피해 발생	21.0
	S-A04-01	22	자폭·폭탄 투하로 연주소 주변 시설 파괴	20.4

위험 대응 우선순위는 실제 대응이 긴급하거나 판단이 필요한 Level A, B, C에 한해 제시하였다. 해당 위험은 수용 불가능 또는 조건부 수용으로 분류되어, 보호체계 구축 시 반드시 고려해야할 위험이다. 이에 따라 모든 해당 위험을 대응 대상으로 전제하되, 위험 수준에 따른 상대적 참고 순서를 함께 제시하였다. 반면 Level D 및 Level E 위험은 상대적으로 위험 수준이 낮아, 방송시설의 자의적 판단이 요구되어 대상에서 제외하였다.

제 6 절 방송시설 위험 대응(Risk Treatment) 단계

1. 방송시설 위험 대응 개요

본 절의 위험 대응 논의는 KS X ISO/IEC 27005에서 제시하는 위험 관리 체계를 기본 방법론으로 준용하되, 표준에서 정의하는 모든 위험 대응 조치를 포괄적으로 검토하는 것을 목적으로 하지는 않는다. 본 연구는 방송시설 보호라는 적용 대상의 특성과 정책 연구의 범위를 고려하여, 안티드론 체계의 구축 및 운용에 따라 위험이 어떻게 변화하고 관리될 수 있는지를 분석 대상으로 한정한다. 이를 통해 방송시설 보호 관점에서 안티드론 체계 도입에 따른 위험 관리 방향을 정책적·운용적 수준에서 검토하는 데 목적이 있다.

2. 위험 대응 전략 정의

본 연구에서의 위험 대응 전략은 개별 위협 시나리오를 완전히 제거하거나, 방송시설의 구조적 변경을 통해 위험을 근본적으로 해소하는 방식이 아니다. 본 연구는 안티드론 체계의 구축 및 운용에 따라 위험 수준이 어떻게 변화하는지를 중심으로 대응 전략을 정의한다.

이에 따라 위험 대응은 위험의 존재 여부를 이분법적으로 판단하는 것이 아니라, 동일한 위협 시나리오가 안티드론 운용 유형에 따라 어느 수준으로 이동하는지를 분석하는 방식으로 설정된다. 즉, 안티드론 체계는 위험을 제거하는 수단이 아니라, 탐지 및 대응 능력의 향상을 통해 위험의 크기와 성격을 관리 가능한 수준으로 이동시키는 관리 수단으로 해석된다.

본 연구는 외부 기관의 관점에서 수행되는 정책 연구로서, 개별 방송시설의 구체적인 대응 절차를 제시하지 않는다. 대신, 기본 방어 수준(운용 유형 1)을 기준선으로 설정하고, 탐지 장비, 소프트킬, 하드킬 도입에 따라 위험 수준이 어떻게 변화하는지를 단계적으로 비교·분석함으로써, 시설관리 주체가 위험 대응 전략을 수립하는 데 참고할 수 있는 판단 근거를 제공한다.

이와 같은 위험 대응 전략 정의는 앞 절에서 도출한 위험 수준 분류 및 위험 대응 우선

순위 결과를 실제 보호체계 구축 논의로 연결하기 위한 전제로서, 이후 절에서는 안티드론 운용 유형별 위험 대응 효과와 한계를 중심으로 분석을 수행한다.

3. 탐지 체계 도입에 따른 위험 수준의 이동

앞서 설정한 위험 대응 전략에 따라, 기본 방어 수준인 운용 유형 1을 기준선으로 하여 탐지 체계 도입에 따른 위험 수준의 변화를 분석하였다. 분석의 초점은 드론 위협에 대한 사전 탐지 능력 확보가 위험 수준 분포에 어떠한 변화를 가져오는지, 그리고 수용 불가 위험의 범위가 어떻게 이동하는지를 확인하는 데 있다. 먼저 운용 유형 2에 해당하는 RF 스캐너 기반 탐지 장비를 도입한 경우는 <표 3-22>과 같다.

〈표 3-22〉 위험 대응 우선 순위 - 운용 유형 2 (RF 탐지)

위험 허용 기준	시나리오 ID	우선 순위	시나리오 설명	위험 수준
수용 불가 Level B	S-A06-07	1	송·중계소 송신 시설 인근 비행, 시설 충돌로 부수적 피해	49.6
조건부 수용 Level C	S-A03-07	2	연주소 송신 시설 인근 비행, 시설 충돌로 부수적 피해	43.4
	S-A05-07	3	송·중계소 수신 시설 인근 비행, 시설 충돌로 부수적 피해	43.4
	S-A03-02	4	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	43.2
	S-A03-01	5	자폭·폭탄 투하로 연주소 송신 시설 파괴	42.0
	S-A05-01	6	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	42.0
	S-A06-01	7	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	42.0
	S-A06-02	8	화염병 등의 위협물 투하, 송·중계소 송신 설비 화재 발생	39.8
	S-A05-02	9	화염병 등의 위협물 투하, 송·중계소 수신 설비 화재 발생	38.4
	S-A02-01	10	자폭·폭탄 투하로 부조정실 구조 손상	25.2
	S-A02-02	11	화염병 등의 위협물 투하로 부조정실 화재 발생	24.6
	S-A01-01	12	자폭·폭탄 투하로 주조정실 구조 손상	24.0
	S-A01-02	13	화염병 등의 위협물 투하로 주조정실 화재 발생	24.0
	S-A05-04	14	불법 정찰로 송·중계소 수신 설비 위치·구조 노출	21.8
	S-A06-04	15	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	21.8

기본 방어 수준에서 식별되었던 수용 불가 위험(Level A 및 Level B)의 분포에 뚜렷한 변화가 나타났다. 운용 유형 1에서는 위험 수준 기준으로 수용 불가(Level A) 8건, 수용 불가(Level B) 1건, 조건부 수용(Level C) 13건의 위협 시나리오가 도출되었으나, 탐지 체계 도입 이후에는 수용 불가(Level B) 1건과 조건부 수용(Level C) 10건으로 재분류되었다.

이는 탐지 체계 도입을 통해 기존에 가장 높은 위험 수준으로 평가되던 시나리오들이 더 이상 '대응이 불가피한 수준'에는 해당하지 않게 되었음을 의미한다. 특히 수용 불가(Level A)에 해당하던 8건의 시나리오가 0건으로 감소함에 따라, 최상위 위험군 기준으로는 실질적으로 전면적인 위험 저감 효과가 나타난 것으로 해석할 수 있다. 다만 여전히 수용 불가(Level B) 또는 조건부 수용(Level C) 수준에 머무르고 있어, 탐지 체계만으로 모든 위험 저감 및 회피의 한계가 있다는 점도 확인되었다.

탐지 체계의 도입은 드론을 직접적으로 차단하거나 무력화하는 수단은 아니다. 그럼에도 불구하고 드론 접근을 사전에 인지할 수 있다는 점은 군·경·전파관리기관 등 관계기관과의 공조 대응을 가능하게 하고, 현장 통제, 인력 대피, 송출 보호 조치 등 비물리적 대응을 선제적으로 수행할 수 있는 기반을 제공한다. 특히 방송시설과 같이 즉각적인 물리적 차단이 곤란한 환경에서는, 탐지 체계 확보 자체가 대응 시간과 선택지를 확대하는 핵심 요소로 기능한다. 이러한 점에서 탐지 체계는 단독 대응 수단이라기보다, 후속 대응을 가능하게 하는 전제 조건으로서 위험 저감에 기여하는 수단으로 해석할 수 있다.

한편 운용 유형 6에 해당하는 레이다 기반 탐지 체계를 적용한 경우에는, 다른 결과가 나타났다. 레이다 탐지는 드론의 항법 방식과 무관하게 탐지가 가능하다는 점에서 탐지 성능 측면에서는 가장 높은 수준의 대응 능력을 제공한다. 그러나 레이다 운용 특성상 능동적인 전파 방사가 수반되며, 이로 인해 기본 방어 수준에서는 존재하지 않았던 전파 간섭 관련 위협 시나리오가 새롭게 도출되었다.

구체적으로 레이다 탐지 체계 적용 시, 프로그램 중계 링크, 이동 중계 링크, 방송서비스 수신 신호 등과 관련된 전파 간섭 시나리오가 조건부 수용(Level C) 수준의 위험으로 새롭게 분류되었다. 이는 레이다 탐지를 통해 드론 접근에 대한 사전 인지 능력은 크게 향상되지만, 동시에 방송시설의 전파 환경 특성상 기존에는 고려되지 않았던 새로운 위험 요소가 추가될 수 있음을 의미한다. 레이다 탐지 체계 도입에 따라 새롭게 발생한 전파 방사 관련 위험 분포는 <표 3-23>과 같다.

〈표 3-23〉 위험 대응 우선 순위 - 운용 유형 6 (레이다 탐지)

위험 허용 기준	시나리오 ID	우선 순위	시나리오 설명	위험 수준
조건부 수용 Level C	S-A14-08	1	프로그램 중계 링크 전파 간섭	25.4
	S-A15-08	2	TV 이동 중계 링크 전파 간섭	25.4
	S-A07-08	3	AM 방송 전파 간섭	21.9
	S-A08-08	4	국제 단파 방송 전파 간섭	21.9
	S-A09-08	5	FM 방송 전파 간섭	21.9
	S-A10-08	6	DMB 방송 전파 간섭	21.9
	S-A11-08	7	디지털 TV 방송 전파 간섭	21.9
	S-A12-08	8	UHD 방송 전파 간섭	21.9

이러한 결과는 탐지 성능의 향상이 항상 위험 저감으로만 이어지는 것은 아님을 보여준다. 특히 레이다 기반 탐지 체계의 경우, 전파 방사로 인한 부수적 위험을 통제하지 않을 경우 조건부 수용 수준의 새로운 위험이 추가될 수 있다. 따라서 레이다 탐지 체계를 방송 시설에 적용하기 위해서는 레이다 운용 주파수와 방송 송·수신 주파수 간의 간섭 가능성이 기술적으로 충분히 배제되어야 하며, 전파 간섭이 발생하지 않음을 전제로 한 주파수 설계 및 운용 검증이 필수적으로 요구된다.

4. 소프트킬 체계 도입에 따른 위험 수준의 이동

본 연구에서는 기본 방어 수준인 운용 유형 1을 기준선으로 하여, 소프트킬 체계 도입에 따른 위험 수준의 이동 양상을 분석하였다. 소프트킬 체계는 탐지 이후 드론의 통신 또는 항법 기능을 교란함으로써 위협을 직접적으로 제어하는 대응 수단으로, 단순 탐지 체계 대비 위험 저감 효과가 보다 명확하게 나타나는 단계이다.

먼저 운용 유형 3에 해당하는 단순 소프트킬 체계를 도입한 경우, 기본 방어 수준에서 수용 불가(Level A 및 Level B)로 분류되었던 주요 위협 시나리오 대부분이 조건부 수용(Level C) 수준으로 이동한 것으로 분석되었다. 시설 인근 공역 비행 이후 충돌로 인한 부수적 피해, 폭발물·위협물 투하에 따른 구조 손상 및 화재 시나리오 등은 위험 수준이 크게 감소하여, 즉각적인 대응이 요구되는 수용 불가 범주에서는 제외되었다. 이는 소프트킬 체계가 드론의 접근 또는 위협 행위를 실제 피해 발생 이전 단계에서 제어할 수 있는 수단

으로 작용함에 따라, 위험의 규모와 긴급성이 완화된 결과로 해석할 수 있다. 단순 소프트킬 체계 도입에 따른 위험 수준 분포는 <표 3-24>과 같다.

〈표 3-24〉 위험 대응 우선 순위 - 운용 유형 3 (단순 소프트킬)

위험 허용 기준	시나리오 ID	우선 순위	시나리오 설명	위험 수준
조건부 수용 Level C	S-A06-07	1	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	28.0
	S-A03-07	2	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	24.5
	S-A05-07	3	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	24.5
	S-A03-02	4	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	24.3
	S-A03-01	5	자폭·폭탄 투하로 연주소 송신 시설 파괴	23.0
	S-A05-01	6	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	23.0
	S-A06-01	7	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	23.0
	S-A06-02	8	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	22.4
	S-A05-02	9	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	21.6
	S-A14-08	10	프로그램 중계 링크 전파 간섭	20.2
	S-A15-08	11	TV 이동 중계 링크 전파 간섭	20.2

다만 운용 유형 3의 단순 소프트킬 체계는 능동적인 전파 방사를 수반하는 특성으로 인해, 기존 기본 방어 수준이나 탐지 체계 단계에서는 존재하지 않았던 새로운 위험을 함께 발생시키는 것으로 분석되었다. 구체적으로 프로그램 중계 링크 전파 간섭과 TV 이동 중계 링크 전파 간섭 시나리오가 조건부 수용(Level C) 수준의 위험으로 새롭게 도출되었으며, 이는 광대역 또는 비정밀 전파 송출 방식에 따른 부수적 영향으로 해석된다. 즉, 단순 소프트킬 체계는 드론 위협 자체에 대해서는 유의미한 위험 저감 효과를 가지는 반면, 방송시설의 전파 환경 측면에서는 추가적인 관리 대상 위험을 수반하는 단계에 해당한다.

반면 운용 유형 4에 해당하는 정밀 소프트킬 체계를 적용한 경우에는 위험 수준의 이동

양상이 보다 뚜렷하게 나타났다. 정밀 소프트킬 체계는 드론 기종 및 통신 특성을 식별한 후 필요한 주파수와 시간에 한정하여 선택적으로 전파를 송출하는 방식으로 운용되며, 이로 인해 단순 소프트킬 단계에서 발생하였던 전파 간섭 관련 위험이 모두 저감 및 회피되는 것으로 분석되었다. 그 결과 운용 유형 4에서는 조건부 수용(Level C) 이상에 해당하는 위험 시나리오가 도출되지 않았으며, 위험 수준 기준으로 모든 위협이 관리 가능한 수준 이하로 이동한 것으로 평가되었다.

이는 정밀 소프트킬 체계가 드론 위협에 대한 직접적인 제어 능력을 유지하면서도, 방송시설의 전파 환경에 미치는 부수적 영향을 효과적으로 억제할 수 있음을 의미한다. 즉, 소프트킬 체계 내에서도 운용 정밀도와 전파 제어 수준에 따라 위험 저감 효과와 신규 위험 발생 여부가 크게 달라질 수 있음을 확인할 수 있다.

5. 하드킬 체계 도입에 따른 위험 수준의 이동

하드킬 체계는 드론을 물리적으로 무력화하는 대응 수단으로, 소프트킬 체계보다 강력한 대응 효과를 가지나, 요격 과정에서 잔존 위협물로 인한 2차 피해 위험이 발생할 수 있다는 점을 함께 고려하였다.

운용 유형 1에서 운용 유형 5로 전환되는 경우, 드론 접근·충돌 및 위협물 투하 등 기존에 높은 위험 수준으로 평가되었던 직접 위협 시나리오는 탐지 이후 요격을 통한 물리적 차단이 가능해짐에 따라 전반적으로 위험 수준이 하향 이동한 것으로 분석되었다. 그 결과 대부분의 시나리오는 조건부 수용(Level C) 이하로 이동하여, 기본 방어 수준에서 나타났던 수용 불가(Level A 및 Level B) 위험 구조는 상당 부분 저감된 것으로 나타났다.

반면, 하드킬 체계 도입과 함께 요격 이후 폭발물에 의한 2차 피해 위험이 새롭게 도출되고, 이는 <표 3-25>과 같다.

〈표 3-25〉 위험 대응 우선 순위 - 운용 유형 5 (하드킬)

위험 허용 기준	시나리오 ID	우선 순위	시나리오 설명	위험 수준
조건부 수용 Level C	S-A03-11	1	요격 후 폭발물이 연주소 송신 시설에 2차 피해	29.0
	S-A04-11	2	요격 후 폭발물이 연주소 주변 시설에 2차 피해	22.0
	S-A05-11	3	요격 후 폭발물이 송·중계소 수신 시설에 2차 피해	22.0
	S-A06-11	4	요격 후 폭발물이 송·중계소 송신 시설에 2차 피해	22.0

즉, 운용 유형 5에서는 하드킬 체계 도입으로 인해 일부 신규 위험이 발생하였음에도 불구하고, 전체 위험 구조를 기준으로 볼 때 위험의 총량은 감소하고, 위험의 성격은 '직접 피해 중심'에서 '통제 가능한 2차 피해 중심'으로 이동한 것으로 해석할 수 있다.

하드킬에 따른 2차 피해 위험은 요격 단계 이전의 탐지 성능과도 밀접하게 연관되어 있다. 드론을 보다 원거리에서 조기에 탐지·식별할 수 있을수록, 요격 지점을 방송 핵심 시설로부터 충분히 이격된 위치로 설정할 수 있으며, 이는 요격 후 폭발물 또는 잔해로 인한 2차 피해 가능성을 구조적으로 감소시키는 요인으로 작용한다. 반대로 탐지 지연 또는 식별 정확도 부족은 요격 시점을 시설 인근으로 제한하여, 하드킬 체계의 부수적 위험을 증폭시킬 수 있다.

따라서, 운용 유형 6으로 확장되는 경우에는, 앞서 소프트킬 체계에서 논의된 전파 방사로 인한 위험 요소를 분석 범위에서 제외하더라도, 탐지·식별·요격이 통합된 고도화된 운용 환경을 통해 대부분의 위협 시나리오가 위험 허용 기준 Level C 이하로 안정화되는 것으로 분석되었다. 특히 하드킬 체계의 운용 정밀도와 대응절차가 성숙될수록, 요격 과정에서 발생 가능한 2차 피해 위험 역시 관리 가능한 범위 내에서 통제될 수 있는 것으로 평가된다.

따라서 하드킬 체계의 위험 평가는 요격 수단 단독의 성능에 국한될 수 없으며, 탐지 범위, 식별 정확도, 대응 여유 시간 등 탐지 체계의 성능 요소를 포함한 통합 운용 관점에서 이루어져야 한다. 이는 하드킬 체계가 고위험 수단이 아니라, 적절한 탐지·통제 조건 하에서 위험을 관리 가능한 수준으로 전환하는 최종 대응 수단으로 기능할 수 있음을 의미한다.

제4장 방송시설 안티드론 시스템 구축 방안

제1절 구축 방안 개요

본 연구에서는 방송시설에서 식별된 위험 요소를 효과적으로 제어하기 위해, 최적의 대응 조치와 기술을 선정하는 체계적인 과정을 수행한다. 이는 단순한 장비의 나열이나 도입을 넘어, 분석된 위협 시나리오에 가장 적합한 기술적 해법을 연결하는 것을 핵심으로 한다.

시스템 구축의 근간은 안티드론 시스템 기반 인프라의 확립에 있다. 이 기반 인프라는 법적·정책적 변화나 내부 운영 환경에 따라 보안 등급을 유연하게 조정할 수 있는 확장성을 갖춰야 한다. 예컨대 VIP 방문, 시상식, 대형 스포츠 경기 등 위험도가 일시적으로 상승하는 상황에서도, 견고한 기반 인프라는 신속하고 효율적인 방어 태세 전환을 보장해야 한다.

결론적으로 본 장의 목표는 고정된 상시 보안 인프라와 상황에 따라 적용 가능한 가변적 대응책을 유기적으로 결합하여, 어떠한 위협 상황에서도 운영의 연속성을 보장하는 빈틈없는 솔루션을 구현하는 것이다.

1. 구축의 절차

안티드론 시스템 구축의 궁극적인 목표는 법적·기술적 한계 내에서 적절한 대응수단을 강구하고, 대상 시설이 직면한 드론 위협 리스크를 효과적으로 완화하는 것이다. 따라서 본 연구에서는 다음과 같은 절차를 통해 구축 방안을 수립한다.

1. 방송 환경의 제약 사항 및 위험 평가를 수행한다.
2. 법적 제약 범위 내에 있는 대응 수준을 선정한다.
3. 선정된 대응 수준에 부합하는 적절한 기술과 솔루션을 선정한다.
4. 운영 프로세스 및 절차를 설계하고 시스템을 구축한다.

먼저 위험 평가 및 목표 설정 단계에서는, 시설의 환경적 특성과 잠재적 위협 시나리오를 분석하여 방어 목표를 수립한다. 시스템 선정 및 설계 단계에서는 법적 제약과 기술적 요구사항(방송 장비 호환성 등)을 고려하여 최적의 장비와 솔루션을 선정한다. 마지막으로 실제 상황 발생 시 적용할 운영 절차(SOP, Standard Operating Procedures)를 확립한다.

본 절에서는 위험 평가를 수행한 이후 법적 검토 단계부터 전체적인 안티 드론 구축 방안을 도출하는 방법과 과정을 기술한다.

2. 시스템 선정 방안

안티드론 시스템의 선정은 단순히 개별 장비의 성능 비교나 기술적 우수성에 근거하여 이루어질 수 없다. 방송시설은 고출력 송신 장비와 복잡한 전파 환경이 결합된 특수한 운용 공간으로 여러 가지 요소를 종합적으로 고려할 필요가 있다. 이에 본 연구에서는 방송시설 환경에 적합한 안티드론 시스템 선정을 위한 각 요소별 고려 사항을 정리한다.

1) 법적 검토

탐지 및 무력화 기술 사용에 대한 허가와 관련된 법적 문제 고려사항이다. 이때 설치 시 방송시설 경계 내외에서 개입할 수 있는 법적 리스크가 무엇인지 조사해야 한다. 이를 위해서는 사법기관, 관계 당국, 인근 주민, 공역 관리, 항공 교통 관리 및 많은 이해 관계자의 참여와 검토가 요구된다.

2) 방어 범위 및 수준

방어 범위와 목표를 명확히 정의하는 것이 중요하다. 이는 과도한 초기 구축 예산 편성과 더불어, 유지보수 비용도 함께 증가 되어 비효율적인 구축이 될 수 있기 때문이다. 따라서 앞서 수행한 위험 분석 결과를 기반으로 실질적인 방어 구역과 요구되는 보안 수준을 구체적으로 설정해야 한다. 하지만 시스템 설계 시에는 초기 구축 단계에서부터 확장성(Scalability)을 필수적으로 고려해야 한다. 이는 향후 위협 양상의 변화에 따라 설정을 유연하게 변경하거나, 새로운 솔루션을 추가 도입 요구를 고려하여야 한다.

3) 부작용 및 영향성

탐지 및 무력화 기술이 주변 환경, 그리고 인접 인프라에 미칠 수 있는 잠재적 영향을 정밀하게 확인해야 한다. 특히 무력화 조치가 초래할 수 있는 부작용에 대해 면밀한 분석이 요구된다.

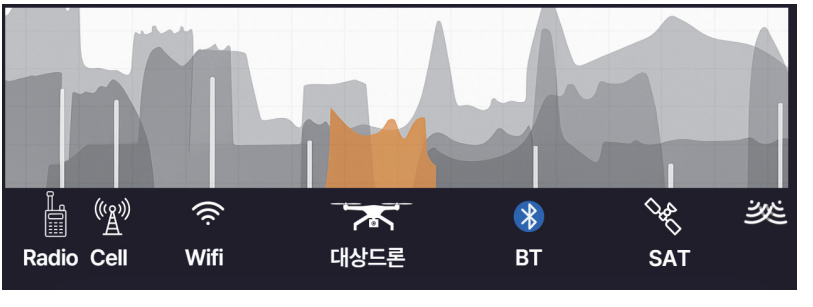
4) 방송시설과의 상호운영성

고출력 송신 장비가 밀집된 방송시설의 특성상, 안티드론 시스템 도입 시 상호 간섭에 의한 탐지 센서의 수신 포화 방지와 방송송출서비스의 연속성 보장이 동시에 요구된다. 따라서 안정적인 상호 운용성을 확보하기 위해서는 방송 장비 및 탐지 장비 모두 전파 간섭을 고려하는 기술적 대책이 필수적으로 강구되어야 한다.

5) 전자기 및 전파 환경 호환성

전자기 간섭(EMI), 무선 주파수 간섭(RFI)은 안티드론 시스템에서 더욱 중요하게 다루어져야 한다. 예를 들어, 자율주행 차량의 라이다(LiDAR)는 안티드론 탐지 자산인 레이다와 혼신을 일으킬 수 있다. 또한 수많은 무선 주파수 간섭은 RF 탐지장비의 혼신을 일으킬 수 있다. 이러한 상호 간섭은 탐지 거리를 단축시키거나, 허위 표적을 생성하여 오탐(False Positive) 및 미탐(False Negative)을 유발하는 주된 원인이 된다. [그림 4-1]은 안티드론의 표적이 되는 일반적인 상용 드론의 주파수 대역과 주변 통신환경을 나타낸다.

〔그림 4-1〕 주변 통신 환경 속 상용 드론의 주파수 대역



3. 시스템 배치 방안

최적의 탐지 범위와 무력화 범위, 그리고 주변 시스템에 대한 안전성을 확보하기 위해서는 적용 대상 센서 및 이펙터의 운용 환경과 잠재적 위협을 종합적으로 분석할 필요가 있다. 안티드론 시스템 구축 시에는 지형, 기상 조건, 주변 장애물 등 물리적 환경 요소가 성능에 결정적인 영향을 미치므로 방어 사각지대를 최소화하고 실제 운용 환경에서의 유효하게 구축해야할 필요가 있다. 본 연구에서는 이러한 조건을 바탕으로, 최적의 방호 범위를 확보하기 위해 시스템 배치 시 고려해야 할 주요 요소를 정리한다.

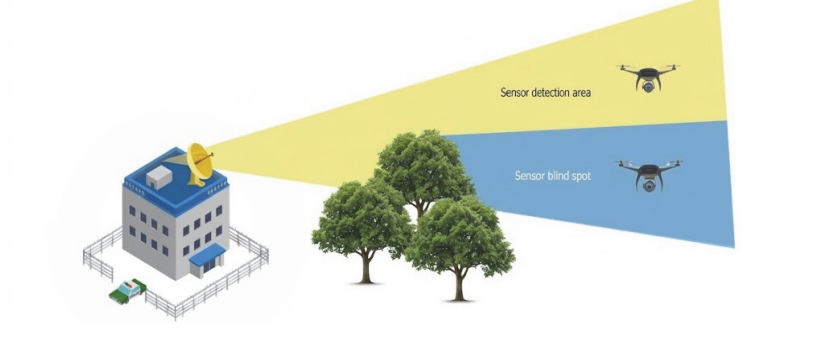
1) 배치 장비 고유의 성능 제원

시스템의 배치 위치는 장비 고유의 성능 제원(Spec)에 의해 결정된다. 단순한 스펙 확인을 넘어, 실제 운용 시 발생할 수 있는 물리적 한계를 극복하기 위해 사각지대를 고려하여 배치를 최적화해야 한다. 방어 범위가 일정 부분 겹치도록 중첩 배치로 구성될 수 있다.

2) 배치 시설의 주변 지형 및 장애물

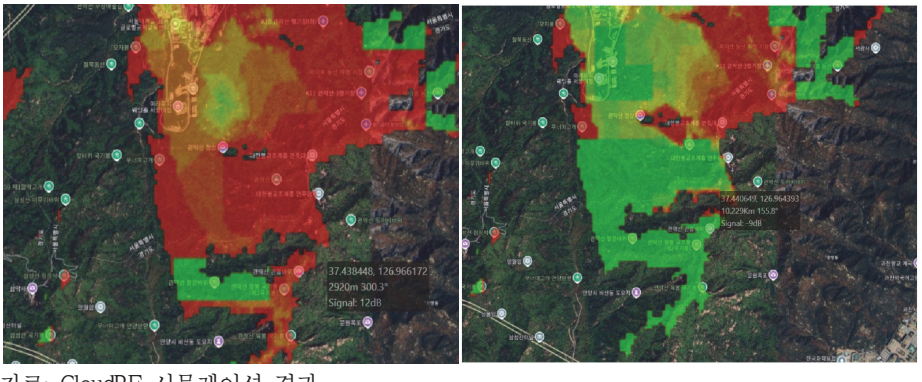
방어 구역 내의 건물, 수목, 산악 지형 등은 센서의 가시선을 제한할 뿐만 아니라, 무력화 장비의 대응 신호, 물리적 매개체 전달을 차단하여 사각지대를 형성하는 치명적인 요인이 될 수 있다. [그림 4-2]는 장애물에 의한 사각지대 발생을 시각적으로 나타낸다.

〔그림 4-2〕 장애물로 인한 사각지대 발생 및 성능 저하



또한 장애물에 의한 신호 감쇠 및 다중 경로 현상은 탐지 좌표의 오차를 유발하여 무력화 장비의 타격 정밀도를 저하시키는 직접적인 원인이 된다. [그림 4-3]은 여의도 지역에서 무력화 장비의 설치 높이에 따라 변화하는 전파 방해 영향을, 관악산 인근의 STL 수신기기를 기준으로 측정한 결과를 나타낸다. 분석 결과, 장비를 주변 지형보다 상대적으로 높은 위치에 설치할수록 무력화 영향 범위는 확대되는 경향을 보였으나, 동시에 STL 수신기기에 대한 전파 간섭 가능성 또한 증가하는 것으로 확인되었다. 따라서 무력화 장비의 설치 높이는 대응 효과와 방송 수신 간섭 위험을 함께 고려하여 설정할 필요가 있다.

〔그림 4-3〕 높은 위치(좌)와 낮은 위치(우)의 전파 방해 STL 1.7GHz 영향 비교



자료: CloudRF 시뮬레이션 결과

3) 배치 시설의 전파 밀집도

도심지의 높은 전파 밀집도는 배경 잡음을 상승시켜 표적 식별을 어렵게 하므로, 시스템 배치 시에는 물리적 차폐 요소를 회피하여 탐지와 무력화의 신호 경로를 모두 확보하고, 사전 스펙트럼 분석을 통해 전파 간섭이 최소화된 최적의 위치를 선정해야 한다.

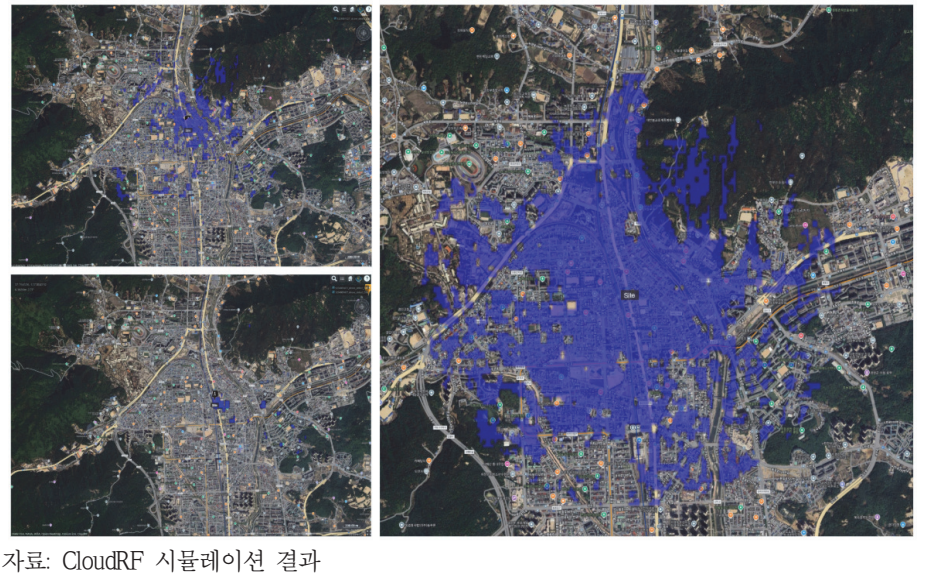
4) 배치 시설의 지원 인프라

시스템 전개 및 운용 유지에 필요한 기반시설을 고려해야 한다. 여기에는 안정적인 전력 공급, 유무선 네트워크 연결 가용성, 그리고 유지보수 인력의 장비 접근성 등이 포함된다.

5) 배치 시설의 설치 환경

탐지 및 무력화 커버리지를 극대화하기 위해서는 기존 인프라(건물 옥상, 통신 마스트, 타워 등)를 적극 활용할 필요가 있다. 특히 방송시설의 경우, 대형 송신 타워나 안테나 구조물이 레이다 및 광학 센서의 물리적 차폐물로 작용하여 심각한 탐지 사각지대를 형성할 수 있다. 이에 따라 구조물로 인한 음영 구역을 상쇄하기 위해 센서를 교차 배치하거나 높이를 올리는 전략이 요구된다. [그림 4-4]은 동일 지역을 대상으로 탐지 장비의 배치 위치(수평적 배치)와 설치 높이(수직적 배치)에 따른 탐지 커버리지 변화를 비교한 결과를 보여준다. 분석 결과, 장비를 단일 지점 또는 낮은 위치에 배치한 경우에는 탐지 음영 구역이 다수 발생한 반면, 기존 인프라를 활용하여 분산 배치하고 높낮이를 달리한 경우에는 탐지 범위가 확대되고 사각지대가 현저히 감소한 것으로 나타났다.

〔그림 4-4〕 장비 배치 및 높이 변경에 따른 서로 다른 탐지 커버리지



자료: CloudRF 시뮬레이션 결과

4. 시스템 운용 방안

안티드론 시스템 운용은 장비의 성능이나 배치만으로 결정되지 않으며, 법적·제도적 책임, 대응 주체의 권한 범위, 외부 기관과의 역할 분담 등을 함께 고려하여 설계될 필요가 있다. 특히 드론 위협 대응은 탐지 이후의 판단과 조치 과정에서 다양한 이해관계자와의 연계를 전제로 하므로, 사전에 운용 구조와 연동 방안을 정리하지 않을 경우 실제 운용 단계에서 혼선이나 책임 문제가 발생할 수 있다. 이에 본 연구에서는 안티드론 시스템 운용 방안 설계를 위해 고려해야 할 주요 요소를 정리한다.

1) 운용 주체와 대응 권한이 일치하지 않는 제도적 환경

방송시설은 드론 위협의 직접적인 피해 대상이지만, 무력화 등 공권력적 대응 권한에는 제도적 제약이 존재한다. 이로 인해 탐지·판단·대응 주체가 분리되는 구조가 형성되며, 운용 단계에서 역할과 책임의 경계를 고려할 필요가 있다.

2) 안티드론 시스템 구성의 이질성과 통합 관리 필요성

방송시설별로 도입 장비의 종류와 탐지 방식이 상이하여, 개별 장비 단위 운용만으로는 위협 상황을 일관되게 관리하기 어렵다. 이에 따라 시설 간 정보 정합성과 통합 관제를 전제로 한 운용 구조 검토가 요구된다.

3) 대응 과정에서 발생할 수 있는 책임 및 면책 문제

안티드론 시스템 운용 중 전파 간섭, 오작동, 2차 피해 등 비의도적 영향이 발생할 수 있으며, 이에 대해 대응의 필요성과 비례성을 사후적으로 검증해야 할 가능성이 존재한다. 이러한 특성은 운용 단계에서 책임 문제를 고려한 구조 설계를 요구한다.

4) 장기 운용 과정에서 발생하는 환경 및 조건 변화

방송시설의 전파 환경, 설비 구성, 운용 인력은 시간에 따라 변화할 뿐 아니라, 드론의 성능·운용 방식 또한 지속적으로 고도화되고 변화한다. 이에 따라 안티드론 시스템은 단기 운용이 아닌, 변화에 대응 가능한 지속 운용 관점을 전제로 검토될 필요가 있다.

제2절 시스템 선정 및 배치

1. 시스템 선정과 이유

방송시설에 적용 가능한 안티드론 시스템은 탐지 및 무력화 기술의 법적 허용 범위, 방송시설 보호를 위해 요구되는 방어 범위와 대응 수준, 기술 운용 과정에서 발생할 수 있는 부작용 및 주변 환경 영향, 방송 장비와의 상호운영성, 그리고 전자기·전파 환경과의 호환성을 종합적으로 고려하여 선정할 필요가 있다. 특히 방송시설은 고출력 송신 설비와 다양한 무선 시스템이 밀집된 환경으로, 드론 대응 과정에서 방송 주파수 간섭이나 송출 장애를 유발하지 않는 것이 핵심 전제 조건으로 작용한다.

이에 따라 본 연구에서는 상기 고려사항을 충족하는 범위 내에서, 법적·운용적 부담이 상이한 세 가지 안티드론 시스템 형태를 도출하고, 각 시스템의 적용 가능성과 한계를 비교·분석하기 위한 기준 모델로 제시한다.

1) RF 탐지, 카메라기반 탐지 시스템

○ 시스템 구성

- RF 스캐너(주파수, 프로토콜)
- 카메라 센서(EO/IR)

○ 선정 이유

- 전파 차단이나 능동적 대응을 하지 않아 현행 법·제도 환경에서 적용 가능성 높음
- 방송시설 경계 외·내부를 포함한 조기 탐지 및 상황 인지 목적에 부합
- 방송 주파수에 직접적인 간섭을 유발하지 않아 송출 연속성 및 전파 안정성 확보

○ 단점

- 드론 탐지 이후 대응은 군·경에 의해서 이루어지므로, 대응이 늦어져 시설 및 인명 피해 가능성 존재

2) RF 탐지, 카메라 탐지기반 정밀 소프트킬 시스템

○ 시스템 구성

- RF 스캐너(주파수, 프로토콜)
- 카메라 센서(EO/IR)
- RF 정밀 소프트킬(스마트 재밍, 정밀제어)

○ 선정 이유

- 무차별 전파 차단이 아닌 정밀 운용으로 인한 법적 제도 회피 가능
- 자폭 드론 등 고위험 위협에 대해 탐지 이후 즉각 대응 수단으로 활용 가능
- 주파수 정합도·운용 시간 제어를 통해 방송 주파수 간섭 최소화 가능
- 전파 혼신 및 부작용 발생 가능성이 존재하여 법적 인증 제도가 필수적

○ 단점

- 드론 탐지 이후 대응은 군·경에 의해서 이루어지므로, 대응이 늦어질 수 있음
- 드론의 항법 방식에 따라 대응 불가 상황 발생

3) 레이다 탐지, 카메라 탐지기반 하드킬 시스템

○ 시스템 구성

- 레이다(방송 미운영 주파수 대역 사용)
- 카메라 센서(EO/IR)
- 하드킬(레이저 등 무력화 시 즉각 요격 가능한 장비)

○ 선정 이유

- 드론의 항법 방식에 의존하지 않고 즉각적인 대응이 가능함

○ 단점

- 물리적 요격을 수반하므로 법적 허용 범위 및 책임 주체가 명확하지 않음
- 요격 잔해, 낙하물 등으로 인한 주변 시설·인명에 대한 2차 피해 가능성 존재
- 방송시설 인근 환경에서 운영 부담 및 사회적 수용성 확보가 어려운 수단

2. 시스템 배치

안티드론 시스템의 배치는 단순한 장비 설치가 아니라, 탐지·무력화 성능 확보와 방송시설 안전성의 균형을 동시에 만족시켜야 하는 설계 문제에 해당한다. 이를 위해 본 연구에서는 앞서 검토한 장비 성능 제원, 지형 및 장애물, 전파 환경, 지원 인프라, 설치 환경을 종합적으로 고려하여 배치 방안을 도출하였다.

특히 방송시설은 고출력 송신 설비와 복잡한 전파 환경이 공존하는 특수한 공간으로 전파 간섭 회피를 핵심 배치 원칙으로 설정하였다. 이러한 원칙에 따라 본 연구에서는 선정한 세 가지 안티드론 시스템 유형별로 다음과 같은 배치 방향을 제시한다.

가. RF 및 카메라 탐지기반 시스템 배치

RF·카메라 기반 탐지 시스템은 방송시설 보호를 위한 기본 탐지 체계로서, 드론 접근을 조기에 인지하고 상황 인식을 확보하는 것을 목적으로 배치된다. 본 연구에서는 시설 규모, 방어 범위, 운용 여건에 따라 단일 세트 구성과 다중 세트 구성의 두 가지 배치 방식을 제시한다. 각 배치 방식은 탐지 범위 설정, 장비 간 연계, 유지관리 여건을 고려하여 상이한 구성으로 설계된다. [그림 4-5]는 RF 스캐너와 카메라를 통합한 단일 세트 장비의 대표적인 배치 예시를 도식화한 것으로, 시설 내 주요 접근 방향을 중심으로 탐지 자산이 배치되는 기본 개념을 보여준다.

〔그림 4-5〕 RF, 카메라 기반 단일 세트 장비 배치 예시

○ 단일 세트 장비 구성 배치

- RF 스캐너와 카메라는 동일 지점 또는 동일 구조물에 통합 배치
- 배치 위치는 시설 중심부 또는 가장 빈번한 드론 접근 방향을 향하도록 설정
- 카메라는 주요 감시 방향을 기준으로 고정 시야 또는 제한 회전 범위로 설정
- 전력·네트워크 접근이 용이하고 상시 유지보수가 가능한 위치를 우선 선정
- 주변 지형에 의한 음영 구역 회피를 위해 장비를 상대적으로 높게 배치
- 단일 장비 배치는 방어 범위를 명확히 한정한 환경을 전제로 적용

○ 다중 세트 장비 구성 배치

- RF 스캐너는 복수 지점에 분산 배치하여 탐지 범위가 상호 중첩되도록 구성
- 카메라는 RF 탐지 범위를 기준으로 교차 감시가 가능하도록 이격 배치
- 대형 구조물, 송신 타워, 지형 장애물로 인한 음영 구역을 상쇄하도록 위치를 분리
- 장비는 동일 구조물 집중 설치를 피하고, 서로 다른 고도·방향을 갖도록 배치
- 주변 지형에 의한 음영 구역 회피를 위해 장비를 상대적으로 높게 배치
- 다중 배치는 [외곽-핵심 자산] 방향으로 단계 감시 구성이 가능하도록 설계

나. RF 및 카메라 탐지기반 정밀 소프트킬 시스템

RF 탐지·카메라 탐지기반 정밀 소프트킬 시스템은 탐지 이후 제한적·선택적인 무력화가 가능한 대응체계로서, 탐지 자산과 무력화 자산 간의 공간적 관계 설정이 배치의 핵심 요소가 된다. 특히 방송시설 환경에서는 무력화 장비의 운용 범위와 방향을 명확히 제한하여, 방송송출설비 및 인접 인프라에 미치는 영향을 최소화하는 배치가 요구된다.

본 연구에서는 이러한 조건을 반영하여, 정밀 소프트킬 시스템의 배치를 단일 세트 구성과 다중 세트 구성으로 구분하고, 탐지-대응 연계 방식과 대응 범위 설정에 따른 배치 방식을 제시한다. [그림 4-6]은 탐지 장비와 정밀 소프트킬 장비가 연계된 다중 세트 배치의 개념적 예시를 나타낸 것이다.

〔그림 4-6〕 탐지 장비 및 정밀 소프트킬 세트 장비 다중 배치 예시

○ 단일 세트 장비 구성 배치

- RF 스캐너, 카메라, 정밀 소프트킬 장비는 탐지-대응 연계가 가능한 동일 지점 또는 인접 구조물에 통합 배치
- 소프트킬 장비는 방송 송신 안테나 및 핵심 전파 설비와 이격된 위치 설치
- 대응 방향은 되도록 시설 외곽 또는 개방 공역을 향하도록 제한
- 소프트킬 장비의 설치 높이는 주변 지형에 따른 전파 감쇠 특성과 인근 수신 설비에 대한 간섭 가능성을 함께 고려하여 조정
- 단일 세트 배치는 제한된 대응 구역에서 선택적 무력화를 전제 환경에 적용

○ 다중 세트 장비 구성 배치

- RF, 카메라 탐지 장비는 다중 분산 배치하여 위협 접근 방향을 조기 식별
- 정밀 소프트킬 장비는 핵심 자산과 일정 거리 이상 이격된 위치에 분산 배치하여 국지 대응 구조로 구성
- 각 소프트킬 장비는 핵심 구역 외곽에 무력화 음영 구역이 없도록 배치
- 무력화 장비의 설치 높이는 주변 지형에 따른 전파 감쇠 특성과 인근 수신 설비에 대한 간섭 가능성을 함께 고려하여 조정
- 다중 세트 배치는 [외곽 탐지-내부 대응]을 분리한 단계적 대응 전제로 설계

다. 레이다 및 카메라 탐지기반 하드킬 시스템

레이다 탐지와 카메라 탐지를 기반으로 한 하드킬 시스템은 물리적 요격을 수반하는 대응체계로서, 운용 범위, 배치 위치, 비용 대비 효율성에 대한 제약이 가장 큰 시스템 유형에 해당한다. 특히 방송시설 환경에서는 요격 범위 내 인접 시설 및 인명에 대한 영향 가능성을 함께 고려해야 하므로, 광범위한 다중 배치보다는 운용 범위를 명확히 한정한 단일 세트 구성이 현실적인 적용 방식으로 판단된다. 또한 장비 단가와 운용·유지 비용을 종합적으로 고려할 때, 다중 세트 배치는 비용 대비 효과 측면에서 적합하지 않은 것으로 평가된다. 이에 따라 본 연구에서는 레이다·카메라 기반 하드킬 시스템을 단일 세트 구성 배치를 전제로 한 배치 방식을 제시한다.

○ 단일 세트 장비 구성 배치

- 레이다와 카메라, 하드킬 장비는 [탐지-식별-무력화] 연계가 가능한 동일 지점 또는 인접 구조물에 통합 배치
- 레이다는 시설 외곽 및 개방 공역을 우선 감시하도록 배치하여, 내부 핵심 자산 방향으로의 전파 방사를 최소화
- 하드킬 장비는 낙하물 및 요격 잔해의 영향을 최소화할 수 있는 방향과 각도로 설치하고, 대응 범위를 명확히 제한

제3절 시스템 운용

1. 시스템 운용 개요

앞서 도출된 시스템 운용 고려 사항을 종합하면, 방송시설 안티드론 시스템은 개별 대응 방식의 선택 이전에 운용 과정 전반에서 준수되어야 할 기준과 원칙을 명확히 설정할 필요가 있다. 이에 본 절에서는 이러한 고려 사항을 반영하여, 외부 기관 연계, 방송시설 간 통합 운용, 사후 분석 및 디지털 포렌식 연계, 유지보수 및 지속 운용의 네 가지 주제에 대해 운용 방식을 제시한다.

2. 외부 협력기관 연동 운용

가. 방송시설 주도 운용 시 외부 협력기관 연동 운용

방송시설이 안티드론 시스템을 직접 운용하는 경우, 역할은 위협의 탐지·인지·상황 판단뿐 아니라 시설 보호 및 송출 안정성 유지를 위한 대응까지 포함하는 것이 현실적이다. 다만 공권력적 조치가 필요한 상황에 대비하여, 외부 협력기관과의 연동은 상황 공유 및 사후 대응 요청 중심으로 구성될 필요가 있다. 이러한 경우의 연동은 다음과 같은 방향을 따른다.

○ 방송시설의 주도 운용

- 안티드론 탐지 시스템을 통해 드론 접근 및 이상 징후를 조기에 인지
- 군·경 등 외부 협력기관에 상황 통보
- 드론의 위치, 이동 경로, 체공 여부 등 정보를 실시간 공유
- 시설 보호 및 방송송출 안정성 유지에 운용의 우선순위를 결정
- 드론 무력화 등 물리적 대응 및 조치를 주도적으로 수행

○ 외부 기관의 보조 운용

- 방송시설로부터 공유된 정보를 기반으로 드론 위협 수준을 판단
- 필요 시 현장 출동 등 사후 대응을 수행

나. 외부 기관 주도 운용 시 방송시설 연동 운용

군·경 등 외부 기관이 드론 대응의 주체로서 안티드론 체계를 운용하는 경우, 방송시설은 직접적인 대응 주체가 아니라 보호 대상이자 현장 정보 제공 주체로서 연동 구조에 참여한다. 이 경우 안티드론 시스템은 방송시설 단독 운용 체계가 아니라, 지역 또는 국가 단위의 공역 대응체계의 일부로 운용되는 형태를 갖는다. 따라서 연동 구조는 외부 기관의 대응 판단을 지원하는 방향으로 설정될 필요가 있다.

○ 방송 시설의 보조 운용

- 안티드론 탐지 시스템을 통해 드론 접근 및 이상 징후를 인지
- 드론의 위치, 이동 경로, 체공 여부 등 현장 정보를 군·경 등 외부 기관에 제공
- 외부 기관의 대응 과정에서 방송송출 안정성, 인력 안전, 시설 보호를 위한 협조 체계 유지

○ 외부 기관의 주도 운용

- 방송시설로부터 제공받은 정보를 기반으로 드론 위협 수준을 판단
- 위협 단계에 따라 소프트킬·하드킬 등 공권력적 대응 여부와 수단을 결정
- 드론 무력화 등 물리적 대응 및 조치를 주도적으로 수행

3. 방송시설 간 통합 운용

방송시설 간 통합 운용은 특정 제조사나 개별 장비에 종속되지 않고, 서로 다른 안티드론 장비를 하나의 운용 체계로 통합하여 관리·관제하기 위한 필수적인 운용 방향이다. 방송시설별로 상이한 탐지·대응 장비가 도입되는 현실을 고려할 때, 개별 장비 단위의 운용이 아니라 공통된 기준과 구조를 통해 장비의 다양성을 통합적으로 관리·운용하는 체계가 요구된다. 이를 위해 방송시설 간 연동은 특정 기술이나 제조사에 종속되지 않는 공통 운용 프로토콜 기반의 통합 관제 체계를 전제로 구성되어야 한다. 국외에서는 이러한 방식이 NATO 등의 표준 제정 기구에서 논의되어 채택된 사례[55]도 존재한다.

55) NATO to adopt SAPIENT as C-UAS standard, JANES, 2023.09.25.

○ 통합 관제 기반 연동 구조의 주요 요소

- 각 방송시설에서 수집되는 탐지 및 상황 정보는 공통 형식으로 변환하여 통합 관제 체계로 수집·관리
- 장비 종류와 관계없이 모든 안티드론 장비의 운용 상태는 동일한 관제 화면과 기준으로 표시·모니터링
- 시설 간 위협 상황은 공통 데이터 구조를 통해 비교·분석할 수 있도록 관리
- 개별 장비의 동작 여부가 아니라, 전체 체계 관점에서 위협 상황을 인지·판단·관리하는 방식으로 운용

4. 사후 분석 및 디지털 포렌식 연계 방안

안티드론 시스템 운용 과정에서 생성되는 탐지 로그, 센서 데이터, 관제 기록 등은 대응의 적정성과 상황 판단의 타당성을 사후적으로 검증하기 위한 기초 자료로 활용될 수 있다. 이에 따라 디지털 포렌식 연계는 방송시설이 수사 또는 법적 판단의 주체가 되는 것을 전제로 하기보다는, 운용 기록을 체계적으로 관리하고 필요 시 외부 기관의 사후 분석을 지원하는 방향으로 운용되어야 한다.

○ 사후 분석 및 디지털 포렌식 연계 운용

- 안티드론 시스템 운용 과정에서 생성되는 탐지 로그, 센서 데이터, 관제 기록을 시간순으로 정리·보존
- 대응 단계 전환 시점, 조치 이력, 외부 협력기관 통보 내역이 사후적으로 확인 가능하도록 관리
- 고위험 위협 또는 반복 발생 사례에 한해, 군·경 등 관계 기관 요청 시 사후 분석 자료를 제공
- 요격·추락·제어권 탈취 등으로 실물 드론을 확보한 경우, 방송시설은 기초 보존 및 인계 역할에 한정하여 외부 기관의 포렌식 분석을 지원
- 방송시설은 수사·법적 판단의 주체가 아니라, 보호 대상이자 객관적 정보 제공 주체의 역할을 유지

방송시설은 안티드론 대응 과정에서 생성되는 정보를 내부 관리 체계에 축적하고, 고위험 또는 반복 위협 사례 발생 시 관계 기관의 사후 분석과 연계될 수 있도록 준비된 상태를 유지할 필요가 있다. 이러한 연계는 방송시설의 법적·제도적 부담을 최소화하면서도, 국가 차원의 위협 분석 체계와 연결되는 구조를 지향해야 한다.

5. 유지보수 및 지속 운용

가. 체계 단위 유지보수 운용

방송시설 안티드론 체계는 시설별로 서로 다른 탐지·관제 장비로 구성될 수 있으며, 이에 따라 유지보수와 점검 역시 개별 장비 단위가 아닌 체계 전반의 운용 상태를 기준으로 접근할 필요가 있다. 이러한 관점에서 체계 단위의 유지보수는 탐지·관제 기능이 일관되게 유지되고 있는지를 중심으로 수행되어야 한다.

○ 체계 단위 유지보수를 위한 운용

- 개별 센서의 정상 동작 여부보다는 체계 전체의 탐지·관제 기능 유지 여부를 기준으로 점검
- 통합 관제 서버와 데이터 연계 기능이 안정적으로 동작하는지 정기적 확인
- 장비 교체 또는 추가 시, 개별 장비 성능보다 체계 연동 상태와 관제 일관성을 우선 점검
- 장비 성능 편차가 전체 탐지·관제 기능에 미치는 영향을 관리 대상으로 설정

나. 운용 환경 변화에 따른 점검 및 보완 운용

방송시설의 전파 환경과 물리적 구성은 시간 경과에 따라 변화할 수 있으며, 이러한 변화는 안티드론 시스템의 탐지 성능과 운용 안정성에 영향을 미칠 수 있다. 이에 따라 안티드론 시스템은 초기 구축 상태를 기준으로 고정 운용되기보다는, 운용 환경 변화를 지속적으로 점검하고 보완하는 관리 관점에서 운용될 필요가 있다.

○ 운용 환경 변화 대응을 위한 운용

- 정기적인 운용 점검을 통해 탐지 범위 및 인지 성능을 확인
- 방송 설비의 증설·변경 등 환경 변화 발생 시 안티드론 시스템에 미치는 영향을 검토
- 오경보 또는 미탐 사례 발생 시 원인을 분석하고 설정을 보완
- 필요 시 탐지 기준이나 관제 설정을 단계적으로 조정

다. 운용 인력 및 절차의 지속성 확보 운용

안티드론 시스템은 장비의 성능 유지뿐 아니라, 이를 운용하는 인력과 절차가 지속적으로 유지될 때 안정적인 운용이 가능하다. 방송시설 환경에서는 인력 순환이나 조직 개편 등으로 인해 운용 경험이 단절될 수 있으므로, 특정 인력에 의존하지 않는 운용 구조를 전제로 관리할 필요가 있다.

○ 운용 지속성 확보를 위한 운용

- 기본적인 시스템 운용 절차와 상황 대응 흐름을 문서화하여 관리
- 관제 화면 해석 방법과 상황 판단 기준을 내부적으로 공유
- 외부 협력기관과의 연동 절차를 정기적으로 점검
- 신규 인력 투입 시 최소한의 운용 이해가 확보될 수 있도록 인수 체계를 유지

제5장 결론 및 시사점

1. 연구 결론

본 연구는 국가중요시설인 방송시설이 직면한 신종 위협인 불법 드론에 대응하기 위해, 체계적인 위험 분석 방법론과 현실적인 구축 전략을 제시하였다. 국제 및 국내 표준에 부합하는 위험 분석·평가 절차를 적용함으로써, 방송시설을 대상으로 한 드론 위협과 이에 대응하기 위한 안티드론 체계가 동시에 내포하는 위험 요소를 구조적으로 검토하였다.

분석 결과, 드론 위협은 의도적인 자폭·투하 공격과 같은 고의적 행위뿐 아니라, 송·수신 안테나 등 핵심 설비와의 우발적 충돌만으로도 방송서비스 중단으로 이어질 수 있는 잠재적 위험을 포함하고 있음을 확인하였다. 아울러 이러한 위협에 대응하기 위한 안티드론 체계 역시 방송시설의 전파·장비 특성에 따라 전파 간섭, 요격에 따른 2차 피해 등 새로운 위험을 유발할 수 있어, 단순한 장비 도입만으로 위험 수준이 일방적으로 감소하지는 않는다는 점을 도출하였다.

이에 본 연구는 방송시설 보호를 위한 안티드론 시스템 구축이 기술 도입 중심의 접근에 머물러서는 안 되며, 장비 운용에 따른 부작용을 고려한 위험 기반 판단과 함께 인증 체계, 정책적 기준, 제도적 보완이 병행되어야 한다.

2. 정책적 및 제도적 시사점

1) 방송시설 안티드론의 안보·법적 공백

현행 법체계상 방송시설은 「통합방위법」에 따라 국가중요시설로 지정되어 있어 드론 위협에 대한 방호 의무를 지닌다. 「방송법」 제85조의2와 「전파법」 제82조는 방송 및 무선설비의 연속적 운영과 보호를 최우선 강행 규범으로 규정하고 있다. 이에 따라 「전파법」 제29조(혼신 등의 방지)에서 국가중요시설 운용에 대한 예외를 일부 인정하고 있음에도 불구하고, 실제 안티드론 대응 시 발생할 수 있는 전파 간섭은 법적 보호를 받지 못하는 실정이다.

이는 방송 관련 법령들은 방송송출의 안정성을 최상위 가치로 두고 있어, 천재지변이나

중대한 재난 상황 등을 제외하고는 방송 중단 또는 제한을 허용하는 ‘정당한 사유’를 극히 제한적으로 해석한다. 현행법상 드론 테러 위협에 대한 방어 행위가 방송 중단을 정당화할 수 있는 사유로 명시되어 있지 않아, 방어 조치로 인한 송출 장애 발생 시 법적 책임 면제가 불가능한 구조다. 이는 기술의 발전 속도를 제도가 따라가지 못하는 전형적인 ‘규제 지체(Regulatory Lag)’ 현상이 지속되고 있다. 결과적으로 현장에서는 드론 방어 장비가 안보상 필요함에도 불구하고 합법적인 대응 수단을 찾을 수 없는 안보적·법적 공백 상태가 지속되고 있다.

2) 정책·제도적 기반의 기술적 안전성 확보 및 표준화 방안

〔그림 5-1〕 방송시설 안티드론 기술적 안정성 확보를 위한 제도적 장치

규제 지체를 해소하고 방송시설의 특수성을 보장하기 위해서는, 추상적인 법적 논쟁을 넘어 ‘기술적 신뢰성’을 담보로 한 ‘제도적 허용’ 전략이 필요하다. 즉, 방송시설 및 인근 전파 환경에 악영향을 주지 않음을 입증한 인증 장비에 한해 운용을 허용하고, 그 설치 및 운용 절차를 표준화하여 법적 리스크를 해소해야 한다. 방송시설에 안티드론을 도입하기 위한 3가지 제도적 장치는 [그림 5-1]과 같다.

가. 방송시설 특화형 안티드론 장비 인증제도 도입

방송시설은 일반적인 국가중요시설과 달리 고출력 전파가 상시 송출되는 특수 환경이다. 따라서 2026년 시행 예정인 안티드론 KS 표준(Korean Industrial Standards)과는 별도로, 민감 전파 환경에 최적화된 안티드론 기자재 적합성 평가의 세부 항목을 신설해야 한다. 예를 들어 방송시설에 대한 안전성을 기술적 입증하여야 한다. 예를 들어 안티드론 장비 가동 시, 방송송출용 주파수 대역에 미치는 간섭이 시간 슬롯과 주파수 슬롯 모두에서 '허용 임계치(Threshold)' 이하임을 스펙트럼 분석을 통해 입증하는 것도 그 방법이 될 수 있다.

나. 물리적·기술적 설치 표준의 의무화

인증된 장비라 하더라도 잘못된 설치는 치명적인 사고를 유발할 수 있다. 따라서 방송시설 내 안티드론 시스템 구축 시 반드시 준수해야 할 엄격한 설치 가이드라인을 제도화해야 한다. 예를 들어, 안티드론 장비와 방송 송신 안테나 간의 최소 물리적 이격거리를 규정하고, 상호 주파수 간섭을 최소화하는 배치 설계를 의무화하거나, 재머(Jammer)나 레이다의 빔 방사 방향이 수신 안테나나 인근 주거 지역을 직접 향하지 않도록, 물리적인 설치를 포함한 시공 기준을 수립한다.

다. 운용 기술 기준 및 사후 관리 제도

설치 이후의 운용 단계에서도 기술적 안전성을 유지하기 위한 관리 제도가 뒷받침되어야 한다. 최초 설치 시의 전파 환경이 유지되고 있는지 확인하기 위해, 연 1회 이상의 정기적인 전파 환경 측정 및 장비 성능 검사를 법적 의무 사항으로 규정한다.

3. 기술적 및 운용적 시사점

1) 자체 방호 원칙과 실질적 대응 권한의 괴리

「통합방위법」상 '자체 방호의 원칙'은 국가중요시설의 관리자(소유자)에게 경비·보안 및 방호에 대한 일차적 책임을 부여하고 있다. 이에 따라 방송시설의 실질적인 방호

수행은 방송사가 고용한 특수경비원 등 민간 보안 조직이 담당하게 된다.

그러나 현행법상 민간 경비 인력은 사법권이 제한적이며, 특히 드론에 대한 물리적·전파적 무력화 권한은 전혀 부여되어 있지 않다. 이로 인해 현장 보안 요원은 위협 드론을 육안이나 장비로 탐지하더라도, 직접적인 대응을 할 수 없어 경찰이나 군에 신고하는 수동적 조치에 그칠 수밖에 없다. 결국, 신고를 받고 공권력이 출동하기까지의 시간차로 인해 드론은 이미 이탈하거나 상황이 종료되는 경우가 빈번하며, 이는 방호 책임자와 실행 권한(경찰·군)의 공백으로 이어져 폭탄 드론 등 고위험 위협 침투 시 즉각적인 초동조치를 불가능하게 만드는 구조적 취약점으로 작용한다.

2) 기술 발전에 따른 법적 운용 권한의 확대 전망

현재 국가가 민간의 안티드론 운용 권한을 엄격히 제한하는 주된 이유는 도심지 내에서의 추락, 전파 혼신 등 부수적 피해(Collateral Damage) 발생 우려 때문이다. 즉, 대응 기술의 불완전성이 법적 규제를 유지시키는 핵심 요인이라 할 수 있다.

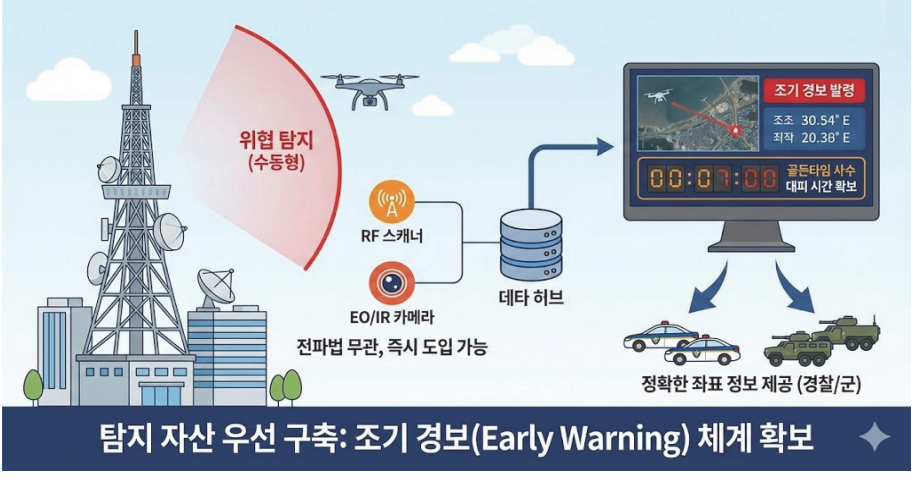
따라서 향후 안티드론 기술이 발전하여 주변 시설이나 인명에 피해를 주지 않는 안전성이 검증되고, 정밀 타격이나 안전한 포획기술이 보편화된다면 상황은 변화할 것이다. 즉 기술적 안전성이 담보된다면, 방송국을 포함한 국가중요시설 관리 주체에게 제한적인 범위 내에서 적극적 방어권(Active Defense Authority)을 부여할 수 있는 법적·제도적 명분이 확보될 것으로 전망된다. 결론적으로, 현재의 제한적인 운용 권한 문제는 부수적 피해가 없는 고도화된 안티드론 기술의 보급과 검증을 통해 자연스럽게 해소될 수 있는 '기술 종속적(Tech-dependent)' 과제라 할 수 있다.

3) 단계적 도입 전략: 탐지 자산 우선 구축 및 민·관·경 원격 협력 운용

법적 운용 권한이 민간에 완전히 이양되기 전까지의 과도기적 공백을 메우기 위해서는, 무(無)대응이 아닌 현행법 내 최선의 대응을 모색해야 한다. 이를 위해 기술적 특성과 법적 제약을 고려한 '투 트랙(Two-Track)' 도입 전략이 시급하다.

가. 전파 자산 무해성을 지닌 탐지 전용 장비의 선제적 도입

〔그림 5-2〕 탐지 자산 우선 구축 : 조기 경보 체계 확보



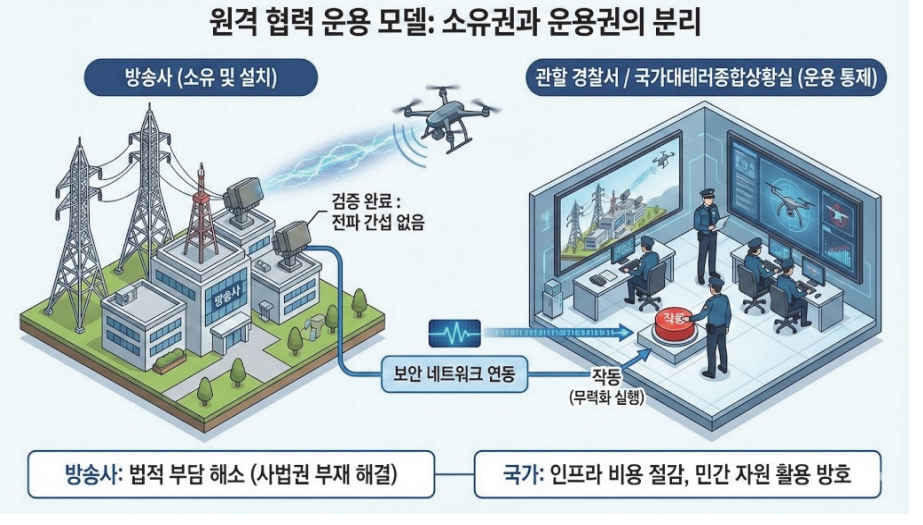
드론 무력화 권한 논쟁과 별개로, 위협을 인지하는 '탐지(Detection) 및 식별(Identification)' 능력 확보는 방호의 기본 전제이다. RF 스캐너(Scanner)나 EO/IR 카메라와 같은 탐지 장비는 전파를 수신하거나 빛을 감지하는 수동형(Passive) 시스템이 주를 이루므로, 전파법상 '혼신'이나 '공격 행위'와 무관하게 즉시 도입이 가능하다. 따라서 [그림 5-2]와 같이 방송시설은 무력화 장비 도입이 지연되더라도 우선적으로 탐지 자산을 구축하여 '조기 경보(Early Warning) 체계'를 갖춤으로써, 위협 발생 시 대피 시간을 확보하고 경찰/군에 정확한 좌표 정보를 제공하여 골든 타임을 사수해야 한다.

나. 인프라 구축(방송사) - 원격 통제(관제센터) 이원화 모델 무력화

무력화(Neutralization) 대응의 경우, "방송 장비에 전파 간섭을 일으키지 않는다"는 기술적 검증이 완료된 장비를 전제로, 소유권과 운용권을 분리하는 '원격 협력 운용 모델'을 제안한다. [그림 5-3]은 원격 협력 운용 모델을 시각적으로 설명한다. 방송사는 자체 예산으로 방송시설 최적 위치에 안티드론 무력화 장비를 설치하고 유지보수를 담당한

다. 운용 통제 등 실제 무력화 기능을 실행하는 작동 권한은 방송사 내부가 아닌, 네트워크로 연동된 관할 경찰서 상황실 또는 국가대테러종합상황실에 부여한다.

〔그림 5-3〕 원격 협력 운용 모델 : 소유권과 운용권의 분리



이는 방송시설 현장에 설치된 장비를 공권력을 가진 법 집행 기관이 관제 등을 통해 상황을 판단한 후 원격으로 작동(Remote Activation)시키는 방식이다. 이 모델을 적용하면 방송사는 직접적인 물리력 행사에 따른 법적 부담(사법권 부재)을 해소할 수 있고, 국가는 별도의 인프라 구축 비용 없이 민간 자원을 활용하여 국가중요시설을 방호할 수 있는 상호 보완적 해결책이 될 것이다.

4. 향후 연구 방향

본 연구는 데이터와 접근 권한의 제약 속에서 시나리오 기법을 통해 논리적 방호 모델을 수립하였으나, 이를 실제 현장에 적용하고 고도화하기 위해서는 다음과 같은 후속 연구가 필수적으로 요구된다. 특히 추상적인 위험 분석을 넘어, 물리적 실체인 ‘안티드론 장비’와 ‘방송 자산’ 간의 상호작용을 과학적으로 규명하는 연구에 집중해야 한다.

가. 안티드론 장비의 방송 자산 영향도에 대한 정량적 · 과학적 실증 연구

본 연구의 가장 시급한 후속 과제는 안티드론 솔루션(특히 재머, 고출력 레이다)이 방송 송출 장비에 미치는 영향을 실험적으로 검증하는 것이다. 시뮬레이션 예측을 넘어, 실제 통제된 테스트베드(Test-bed) 환경에서 장비별 주파수 간섭, 고조파(Harmonics) 영향, 전자기적 내성(EMS) 등을 측정해야 한다. 이를 통해 방송 장비별 안전 이격 거리(Safe Separation Distance)와 주파수 대역별 허용 출력 임계치(Power Threshold)를 수치적으로 산출하고, 어떤 장비를 어디에 설치해야 방송사고 없이 드론을 막을 수 있는가에 대한 과학적 기준 데이터(Reference Data)를 확보해야 한다.

나. 위협 데이터베이스(DB) 구축 및 정량적 확률 모델 개발

현재의 '정성적 시나리오 분석'에 더해 '정량적 확률 분석'을 반영한다. 이를 위해서는 방송시설 인근의 드론 비행 로그(Log)를 체계적으로 수집 · 축적해야 한다. 탐지 장비를 시범 도입하여 연간 드론 출몰 횟수, 비행 고도, 기종 식별 정보 등을 데이터베이스화(DB)하고, 이를 기반으로 통계적 기법을 적용하여 침투 확률 및 침투 경로를 예측하는 연구로 나아가야 한다. 누적된 데이터를 통해 위험 평가의 정확도를 높이고, 비용 대비 효과(ROI)를 수치로 증명할 수 있는 객관적 토대를 마련해야 한다.

다. 내부 자산 데이터를 반영한 현장 밀착형 분석

본 연구에서 제시한 분석을 바탕으로, 실제 방송시설의 내부 보안 담당자가 참여하는 '현장 검증(Field Validation)' 연구가 수행되어야 한다. 외부 연구자가 접근할 수 없었던 은폐된 자산, 사각지대, 상세 전력망 도면 등 기밀(Confidential) 데이터를 모델에 대입하여, 해당 시설에 특화된 최적 배치 시뮬레이션을 수행해야 한다. 이 과정에서 일반 모델과 실제 현장 간의 괴리를 분석하고 보정함으로써, 연구 결과의 실무 적용성을 최종적으로 완성해야 한다.

라. 안티드론 운용 전문성 확보 및 거버넌스 체계 수립 연구

기술적 도입 및 운용 권한뿐만 아니라, 이를 운용할 '사람' 혹은 '조직'과 절차에 대한 연구가 병행되어야 한다. 이를 기반으로 직무 교육 커리큘럼을 개발하고, 민·군·경 협력 운용 시의 명확한 지휘 통제(C2) 절차와 교전 규칙(ROE)을 표준화하는 '안티드론 운영 거버넌스(Governance)' 연구가 지속적으로 이루어져야 한다.

5. 맺음말

방송시설의 안티드론 시스템 구축은 그 자체가 가지는 민감성 때문에, 단순 장비 도입 및 운용이 아닌, 위험 분석-최적 설계-제도적 보완 이 어우러진 종합적인 관점에서 접근해야 한다. 방송시설 안티드론 시스템은 현재 기술 수준으로 구축과 운영에 일정 부분 어려움이 따르는 것이 사실이나, 시설 자체가 지닌 민감성을 고려할 때 단순한 장비 도입을 넘어 위험 분석, 최적 설계, 제도적 보완이 조화를 이루는 종합적인 관점의 접근이 반드시 필요하다. 본 연구가 제시한 위험 분석 프레임워크와 정책적 제언이 중단 없는 방송서비스와 빈틈없는 국가 중요시설 방호라는 궁극적 목표를 달성하는 데 기여하기를 기대한다.

참 고 문 헌

국내 문헌

[1] 박일송.나종남 (2015),『하이브리드 전쟁(Hybrid War): 새로운 전쟁 양상?』, 한국군사학논집.

[2] 곽해용 (2021),『국가중요시설 Anti-Drone 시스템 구축에 관한 실증연구: 계층분석 기법을 중심으로』, 고려대학교 기술경영전문대학원 박사학위논문.

[3] 송채근.김형석 (2025),『드론위협 대응을 위한 국가중요시설의 방호 전략 연구』, 한국대드론산업학회지.

[4] 김태영.최연준 (2020),『드론 테러 위협에 대비한 국가중요시설 방호체계 개선방안 연구: 물리보안 위험평가모형을 중심으로』, 한국치안행정논집.

[5] 황순필.김주환 (2020),『국가중요시설 방호를 위한 안티드론 시스템 구축 방안 연구』, 디지지털융복합연구.

[6] 이유빈.류세환.윤진섭 (2023),『수자원시설 방호를 위한 안티드론시스템 구축방안 연구』, 대한토목학회 학술대회.

[7] 이동진.정길현.권형안.양상운 (2021),『디지털 트윈 기반 안티드론 시스템 구축 방안』, 한국국방기술학회지.

[8] 정종운.이창한.이태명 (2020),『드론 확산에 따른 국회 안티드론방어체계 구축방안』, 한국경호경비학회.

[9] 하충수 (2023),『국가중요시설에 대한 북한의 드론테러 위협 분석을 통한 대응방안 연구』, 한국재난정보학회 논문집.

[10] 이세훈 (2018),『지상파 방송은 어떠한 경로로 전달되는가?』, 월간 방송과기술.

[11] 이아름 (2017),『드론 시장 및 산업 동향』, 융합연구정책센터.

[12] 시그마프레스,『드론의 구성』, 시그마프레스

[13] 항공안전기술원 (2021),『2021 국내외 드론산업동향 분석』, 항공안전기술원.

[14] 김문국.신인태.이재국 (2023),『현대 전쟁에서의 드론 역할 분석을 통한 차세대 드론

발전 방향 연구: 걸프 전쟁부터 우크라이나 전쟁까지를 중심으로』, 한국산학기술학회논문지.

[15] 김성한.김태홍.최주평.권호진.이재성.권재광.서범규 (2021),『안티드론시스템 연구・시험을 위한 야외시험장 구축 타당성 연구』, 미래전파공학연구소.

[16] 장민재 (2021),『드론 테러 위협의 문제점과 대응방안』, 국내석사학위논문 용인대학교 일반대학원.

[17] 이동혁.강욱 (2019),『안티드론 개념 정립 및 효과적인 대응체계 수립에 관한 연구』, 한국경호경비학회.

[18] 오일석 (2023),『안티드론(Anti-Drone) 정책 발전 방안』, 국가안보전략연구원.

[19] 이인재.최상혁.주인원.전진우.차지훈.안재영 (2022),『불법 드론 대응을 위한 저고도 드론 탐지 기술 동향』, 전자통신동향분석.

[20] 윤경화 (2021),『델파이 기법을 활용한 안티드론 산업 정책평가 지표 개발』, 국내박사학위논문 건국대학교 대학원.

[21] 최상혁.채종석.차지훈.안재영 (2018),『안티 드론 기술 동향』, 한국전자통신연구원.

[22] 변용진.이상수 (2024),『Robotic Warfare 다가오는 무인화 전쟁의 시대』, iM증권 리서치본부.

해외 문헌

[23] Martin Kitchen (2015). “Speer: Hitler’s Architect.” Yale University Press.

[24] Viktoriia Boiko, Alona Stadnyk, Nataliia Polovaia, Olena Vaniushyna, Olena Khodus, Tetiana Ivanets(2022). “USING MEDIA AS WEAPONS IN HYBRID WAR”, pp.175 ~ 179.

[25] Philip Butterworth-Hayes (2023). “The Counter UAS Directory and Buyer’s Guide” Counter UAS DIRECTORY.

[26] Federal Aviation Administration, Department of Justice, Federal Communications Commission & Department of Homeland Seurity (2020). “Advisory on the Applicaion of Federal Laws to the Acquisition and Use of Technology to Detect

and Mitigate Unmanned Aircraft Systems" United States Government.

[27] RON JOHNSON (2018). "Committee on Homeland Security and Governmental Affairs" U.S Government Publishing Office.

[28] U.S. House of Representatives, Committee on Rule (2025). "Rules Committee Print 119-16: Text of House Amendment to S. 1071 (National Defense Authorization Act for Fiscal Year 2026)"

[29] EASA (2019). "EASA Counter Drones(C-UAS) action plan" ECTRL workshop.

[30] Civil Aviation Authority (CAA) (2025). "Unmanned Aircraft Systems Delegated Regulation" UK Regulation (EU) 2019/945.

[31] Civil Aviation Authority (CAA) (2025). "UAS Regulation" UK Regulation (EU) 2019/945.

[32] Sunil Naik (2005). "Hitless Space Diversity STL Enables IP+Audio in Narrow STL Bands" Moseley.

부 록

1. 방송시설 대상 위험 기준 산정

본 연구는 방송시설을 둘러싼 위험 분석에 영향을 미치는 주요 고려 요소를 정리하였다. 본 절에서는 이러한 검토 결과를 바탕으로, 이후 위험 분석과 위험 평가 단계에서 일관되게 적용할 수 있는 위험 기준(Risk Criteria)을 구체적으로 도출한다. 위험 기준은 드론 위협이 방송시설에 미치는 영향을 어떠한 관점과 척도로 판단할 것인지에 대한 공통의 판단 틀을 제공하는 역할을 한다.

이에 따라 본 연구는 위험 기준을 영향도(Impact)와 발생 가능성(Likelihood)의 두 요소로 구성하고, 먼저 드론 위협으로 인해 발생할 수 있는 피해 수준을 판단하기 위한 영향도 기준을 설정한다.

1) 영향도 기준 설정

위협으로 인해 방송시설이 받게 되는 영향은 단일 요인으로 설명되기 어렵다. 방송서비스의 연속성은 전파 혼신, 물리적 충돌, 장비 손상 등 다양한 형태의 위협에 의해 직접적으로 저해될 수 있으며, 이러한 영향은 방송송출 중단이라는 형태로 즉시 나타날 수 있다. 한편, 동일한 위협은 방송 인프라 설비의 물리적 파괴나 현장 안전 위험과 같은 물리적 피해로 확산되어, 서비스 중단과는 다른 양상으로 방송시설에 영향을 미칠 수 있다.

이와 같은 특성을 고려하여 본 연구에서는 위협으로 인한 영향을 서비스 중단 영향(DoS, Denial of Service)과 인프라와 인명 피해 영향의 두 축으로 판단되는 안전 영향을 영향도 평가 기준을 설정하였다. 서비스 중단 영향은 방송송출 및 운용의 연속성에 미치는 직접적인 영향을 의미하며, 방송서비스의 중단 시간과 영향 범위를 중심으로 평가한다. 서비스 중단 영향에 대한 단계별 기준은 <표 6-1>과 같이 정의한다.

〈표 6-1〉 서비스 중단 영향도 산정 기준

수준	서비스 중단 영향(DoS)	점수
Level 1 매우 경미	1분 미만의 지연 또는 미세한 품질 저하, 또는 방송서비스 영향 없음, 즉시 복구 가능	1점
Level 2 경미	1~10분 미만의 단기 중단 또는 간헐적 끊김	2점
Level 3 중간	10분 ~ 1시간 미만 서비스 영향, 지역 단위 품질 저하	3점
Level 4 심각	1시간 이상 ~ 수 시간 서비스 중단, 광역 영향 가능	4점
Level 5 치명적	수 시간 ~ 수 일 이상 중단 또는 정상화 불가	5점

한편, 안전 영향은 방송서비스의 즉각적인 중단 여부와는 별도로, 위협으로 인해 방송시설이 물리적으로 입을 수 있는 피해와 안전 위험을 평가하기 위한 기준이다. 본 연구에서 인프라·안전 영향은 연주소, 송신국, 중계소 등 방송 인프라 설비 자체의 물리적 손상 정도와 방송시설 내 또는 인접 영역에서 발생할 수 있는 인명 안전 위험으로 한정하여 정의한다. 민간 통신 장애, 사회적 혼란, 여론 악화와 같은 비물리적·사회적 파급효과는 평가 범위에 포함하지 않는다. 인프라·안전 영향에 대한 단계별 기준은 〈표 6-2〉, 〈표 6-3〉과 같다.

〈표 6-2〉 인프라 파괴 영향도 산정 기준

수준	인프라 파괴 영향 기준	점수
Level 1 매우 경미	방송 인프라 설비 손상 없음	1점
Level 2 경미	비핵심 방송 설비의 경미한 손상 또는 후속 피해 위험 증가	2~4점
Level 3 중간	핵심 방송 설비 일부 손상 또는 성능 저하	5~6점
Level 4 심각	주요 방송 인프라 손상(송신기, 안테나, 제어 설비 등)	7~8점
Level 5 치명적	방송 인프라의 구조적 또는 전면적 파괴	9~10점

〈표 6-3〉 인명 피해 영향도 산정 기준

수준	인명 피해 영향 기준	점수
Level 1 매우 경미	인명 안전 위험 없음	1점
Level 2 경미	경미한 안전 위험 존재	2점
Level 3 중간	중상 가능성 존재	3점
Level 4 심각	중대 안전사고 발생 가능	4점
Level 5 치명적	인명 피해 발생 가능성 매우 높음	5점

안전 영향 평가에서 인프라 파괴와 인명 피해 영향을 분리하여 정의한 이유는, 두 요소가 방송시설 보호 관점에서 갖는 중요도와 영향 양상이 서로 다르기 때문이다. 인프라 파괴는 연주소, 송신국, 중계소 등 방송시설의 핵심 설비에 대한 물리적 손상을 의미하며, 설비의 손상 정도에 따라 복구 소요 시간, 대체 수단의 존재 여부, 장기적인 방송서비스 안정성에 미치는 영향이 크게 달라진다. 특히 송신기, 안테나, 제어 설비와 같은 핵심 인프라의 손상이나 파괴는 단기간 복구가 어렵고, 광역적인 방송서비스 중단으로 이어질 가능성이 높다는 점에서 방송시설 보호 측면에서 가장 중대한 피해 요인으로 작용한다.

이에 본 연구에서는 인프라 파괴 영향을 인명 피해 영향보다 상대적으로 높은 비중으로 반영하기 위하여, 인프라 파괴 점수를 최대 10점까지 부여하도록 설정하였다. 이는 방송시설 보호를 목적으로 하는 본 연구의 특성을 반영한 것으로, 인프라 설비의 손상 여부와 그 수준이 전체 피해 규모를 결정하는 핵심 요인임을 고려한 결과이다. 반면, 인명 피해 영향은 인명 피해 및 안전사고 발생 가능성을 평가하기 위한 지표로서 중요하지만, 방송시설 보호 관점에서의 직접적인 서비스 지속성 및 설비 복구 가능성에 미치는 영향은 인프라 파괴에 비해 상대적으로 제한적이므로 최대 5점 범위로 설정하였다.

인프라 파괴 점수와 인명 피해 영향 점수는 단순 합산하지 않고, 가중치를 반영하여 하나의 안전 영향도로 환산한다. 이를 통해 인프라 파괴의 중요도를 충분히 반영하면서도, 인명 피해 영향이 전체 평가에서 적절히 고려될 수 있도록 하였다. 안전 종합 영향도는 다음의 수식에 따라 산정한다.

$$영향도_{안전} = \frac{영향도_{인프라} + 영향도_{인명}}{3}$$

해당 산정식은 인프라 파괴와 인명 피해 영향을 결합한 결과가 최대 5점 범위로 정규화되도록 설계되어, 서비스 중단 영향도와 동일한 척도에서 비교·분석이 가능하도록 한다.

$$영향도_{드론위협} = 영향도_{서비스중단} + 영향도_{안전}$$

마지막으로, 서비스 중단의 영향도와 안전 영향도를 합산하여 최대 10점 범위로 방송시설 피해를 전체적으로 고려할 수 있도록 하였다. 이러한 영향도 산정 방식은 복합적인 피해 양상을 보이는 드론 위협 시나리오에 대해 일관된 기준으로 영향 수준을 평가하기 위한 기초 도구로 활용된다.

2) 발생 가능성 기준 설정

본 절에서는 도출된 위협 시나리오가 실제 방송시설 운용 환경에서 현실적으로 발생할 가능성을 평가하기 위한 기준을 설정한다. 본 연구에서 발생 가능성은 단순한 확률값이 아니라, 공격 실행에 필요한 조건의 성숙도와 시설이 보유한 방어·대응 수준이 결합된 결과로 정의한다. 즉, 드론 위협이 기술적·환경적 측면에서 얼마나 용이하게 실행될 수 있는지와, 해당 위협이 방어체계에 의해 얼마나 효과적으로 통제될 수 있는지를 종합적으로 고려하여 판단한다. 이에 따라 본 연구에서는 발생 가능성 평가를 드론 기반과 안티드론 기반의 두 가지로 구분하여 기준을 설정하였다.

① 드론 위협 발생 가능성

드론 위협 발생 가능성은 공격자가 해당 위협을 실제로 실행할 수 있는 조건의 성숙도와, 이를 통제할 수 있는 방송시설의 방어·대응 수준을 종합적으로 고려하여 평가한다. 본 연구에서는 발생 가능성을 단일 요소가 아닌, 공격 실행 조건과 방어 수준이 결합된 결과로 정의하고 비교 가능한 형태로 구조화하였다. 먼저 공격 실행 조건은 다음 네 가지 요소를 중심으로 평가한다.

○ 공격 실행 조건

- 기술적 진입장벽
- 공격 자산 획득성
- 표적 정보 노출도
- 물리적 접근성

각 요소는 공격자가 위협을 실행하기 위해 극복해야 할 난이도를 의미하며, 점수가 높을수록 공격 실행이 용이함을 나타낸다. 발생 가능성 평가의 일관성을 확보하기 위해, 본 연구에서는 공격 실행 조건을 5단계로 구분하고, 각 Level을 1~10점의 점수 구간과 연계하여 정의하였다. 공격 실행 조건에 따른 발생 가능성 산정 기준은 다음 <표 6-4>과 같다.

〈표 6-4〉 공격 실행 가능성 산정 기준

수준	기술적 수행 용이성	공격 자산 획득성	표적 정보 노출도	물리적 접근성	점수
Level 1 매우 낮음	특수 조직급 수준 요구	국가급·통제 장비 필요	고도 기밀 정보 필요	물리적 접근 거의 불가	1~2점
Level 2 낮음	고급 전문 기술·훈련 필요	고난도 확보 수단 요구	기밀 수준 정보 필요	접근 난이도 매우 높음	3~4점
Level 3 보통	전문 기술 인력 필요	특수 장비 확보 필요	비공개 정보 기반	복합 차단 구조 존재	5~7점
Level 4 높음	숙련자 수준 기술 요구	자작·개조 장비 확보 가능	제한적 정보 접근 필요	단순 차단 구조 존재	8~9점
Level 5 매우 높음	초보자 수준 수행 가능	상용 장비 즉시 확보 가능	공개 정보만으로 식별 가능	물리적 차단 요소 없음	10점

기술적 수행 용이성은 해당 공격을 수행하기 위해 요구되는 조종 숙련도, 운용 경험, 기체 및 페이로드 개조 필요성 등을 종합적으로 고려하는 항목이다. 자동 비행 및 안정화 기능이 적용된 상용 드론은 초보자도 단기간 내 운용이 가능하므로 기술적 수행 용이성이 높은 시나리오로 평가될 수 있는 반면, FPV 드론과 같이 고도의 조종 숙련도를 요구하는 경우에는 상대적으로 낮은 기술적 수행 용이성을 갖는 것으로 해석된다. 또한 특정 위협 시나리오 수행을 위해 기체 구조 변경이나 탑재물 개조가 필요한 경우 기술 난이도 평가 항목에 포함된다.

공격 자산 획득성은 공격 수행에 필요한 드론 기체 및 페이로드를 확보하는 데 요구되는 난이도를 의미한다. 상용 드론이나 범용 부품을 활용한 자작 장비는 획득 난이도가 낮은 반면, 특수 제작 장비나 고도의 기술적 완성도를 요구하는 자산은 상대적으로 획득 난이도가 높은 것으로 평가된다.

표적 정보 노출도는 방송시설 또는 개별 설비의 위치, 구조, 운용 정보가 외부에 어느 정도 공개되어 있는지를 판단하는 기준이다. 지도 서비스나 공개 자료를 통해 일반인이 쉽게 접근 가능한 정보는 공개 정보 수준으로 평가되며, 제한된 자료를 통해서만 파악 가능하거나 추가적인 현장 정찰이 필요한 경우에는 정보 노출도가 낮은 것으로 평가된다.

물리적 접근성은 공격 대상 설비가 외부에 노출되어 있는지, 또는 차단 구조나 밀폐 환경에 의해 보호되고 있는지를 기준으로 판단한다. 외부 노출 설비는 접근성이 높은 반면, 단일 또는 다중 차단 구조, 실내 설치 설비 등은 접근 난이도가 점진적으로 증가하는 것으로 평가된다.

한편, 동일한 공격 실행 조건을 갖는 시나리오라 하더라도, 시설이 보유한 방어체계 수준에 따라 실제 위협의 발생 가능성은 크게 달라질 수 있다. 이에 본 연구에서는 공격 실행 조건 평가 이후, 방어 수준을 발생 가능성 산정의 조정 변수로 적용한다. 방어 수준은 탐지·식별·대응·통제 능력의 구축 정도에 따라 구분하며, 수준이 높을수록 실제 위협 발생 가능성은 감소하는 것으로 해석한다. 방어 수준에 대한 기준은 <표 6-5>과 같다.

〈표 6-5〉 방어 수준 산정 기준

수준	정의	방어 수준	점수
Level 1 매우 낮음	무방비	드론 탐지·식별·대응 체계 부재 육안 관찰 또는 사후 인지 수준에 의존	1점
Level 2 낮음	단순 감시	CCTV 등 비전용 감시 수단만 존재 드론 탐지·식별 불가, 실질적 통제 불가능	2점
Level 3 보통	제한적 탐지	전용 드론 탐지 수단 일부 보유(RF 또는 레이다 단일 센서 등), 탐지는 가능하나 즉각 대응은 곤란	3~5점
Level 4 높음	부분 대응	다중 센서 기반 탐지 및 제한적 대응 수단 보유 상황 인지·경보·부분 통제 가능	6~8점
Level 5 매우 높음	다층 방어	탐지·식별·추적·대응이 연계된 다층 방어체계 구축 상시 관제 및 기관 연계 대응 가능	9~10점

본 연구에서는 드론 위협 시나리오의 발생 가능성을 평가하기 위해, 먼저 공격자가 실제로 위협을 실행할 수 있는 조건을 정량화한다. 공격 실행 가능성은 기술적 수행 용이성, 공격 자산 획득성, 표적 정보 노출도, 물리적 접근성의 네 가지 요소를 기준으로 평가하며, 각 요소에 대해 동일한 10점 척도의 점수를 부여한다. 이후 네 요소의 평균값을 산출하여 공격 실행 가능성 점수로 정의한다.

이에 따라 공격 실행 가능성은 다음 식과 같이 산정된다.

$$\text{발생가능성}_{\text{공격실행}} = \frac{\text{기술적 난이도} + \text{공격자산 획득성} + \text{표적 정보노출도} + \text{물리적 접근성}}{4}$$

다만 공격자가 위협을 실행하기에 유리한 조건을 갖추고 있더라도, 시설에 구축된 방어·대응 체계의 수준에 따라 실제 위협 발생 가능성은 달라질 수 있다. 본 연구에서는 이러한 방어 효과를 발생 가능성 산정에 반영하기 위해, 방어 수준을 최종 조정 변수로 적용한다.

구체적으로 방어 수준 점수가 높을수록 무력화 및 대응 능력이 강화된 것으로 간주하여, 공격 실행 가능성 점수를 비선형적으로 감쇠하는 방식을 적용한다. 이를 통해 탐지 중심의 방어 수준과 무력화 중심의 고도화된 방어 수준 간 차이가 발생 가능성에 보다 명확히 반영되도록 하였다.

이에 따라 드론 위협의 최종 발생 가능성은 공격 실행 가능성 점수에 방어 수준 기반 감쇠 계수를 적용하여 다음과 같이 산정한다.

$$\text{발생가능성}_{\text{드론 위협}} = \text{발생가능성}_{\text{공격 실행}} \times ((11 - \text{방어 수준})/10)^2$$

② 안티드론 시스템 운용에 따른 부작용 시나리오의 발생 가능성

안티드론 시스템은 드론 위협을 통제하기 위한 방어 수단이지만, 운용 방식과 기술적 특성에 따라 전파 혼신, 비의도적 신호 간섭, 드론 추락 등 다양한 형태의 부작용 위험을 동반할 수 있다. 특히 방송시설은 전파 기반 설비의 밀집도가 높고, 주파수 운용의 연속성과 안정성이 중요한 환경적 특성을 가지므로, 안티드론 시스템 운용으로 인한 부작용은

방어 효과와는 별도로 독립적인 위험 요인으로 평가될 필요가 있다.

이에 본 연구에서는 안티드론 시스템 운용에 따른 부작용 발생 가능성을 무력화 방식의 기술적 특성에 따라 구분하여 분석한다. 즉, 전파 방출을 기반으로 하는 소프트킬 방식과 물리적 무력화를 전제로 하는 하드킬 방식은 부작용의 발생 메커니즘과 양상이 상이하므로, 각각을 구분된 부작용 시나리오로 설정하여 발생 가능성을 평가한다.

○ 전파 방사의 부작용 발생 가능성

전파 방사는 레이다 탐지, 재밍・스푸핑 등을 통해 드론의 통신・항법 기능을 교란하는 방식으로, 물리적 충돌이나 파편 발생을 수반하지 않는다는 장점을 가진다. 그러나 전파 방사 특성상 의도하지 않은 전파 성분이 확산되어 방송 신호 또는 인접 통신시스템에 혼신을 유발할 가능성이 존재한다. 특히 방송시설은 전파 환경이 복합적으로 구성된 시설이므로, 전파 방사에 따른 부작용 발생 가능성을 기술적 관점에서 평가할 필요가 있다.

본 연구에서는 전파 방사 부작용 발생 가능성을 전파 방사의 정밀성과 방사 특성의 두 관점에서 구분하여 평가하였다. 정밀성은 목표 드론 통신 특성과의 정합 정도를, 방사 특성은 송출 전력, 안테나 지향 특성, 불요파 발생 가능성 등 전파 확산과 관련된 물리적 조건을 의미한다. 이에 따라 본 연구에서는 전파 방사 부작용 발생 가능성을 다음의 다섯 가지 기술적 요소로 구분하여 정의하였다.

[정밀성]

- 주파수 정합도(드론 통신 채널・대역폭에 대한 차단 범위의 선택성/정밀성)
- 시간 정합도(필요 시 송출 여부, 송출 지속성 및 운용 방식)

[방사 특성]

- 불요파 억제력(스퓨리어스, 하모닉스 등의 억제 수준)
- 전파 방사 각도(빔 폭, 방향 기준)
- 전력 세기(송출 전력 규모)

이 중 주파수 정합도와 시간 정합도는 전파 방사가 목표 드론의 통신 특성에 얼마나 선택적으로 정합되어 운용되는지를 나타내는 요소로, 부작용 발생 가능성에 미치는 영향도가 크다. 차단 대상 주파수와 무관하게 대역 전체를 송출하거나 장시간 전파를 지속 송출

하는 경우, 방송 신호 및 인접 통신시스템에 혼신을 유발할 가능성이 크게 증가한다.

이에 본 연구에서는 주파수 정합도와 시간 정합도를 전파 방사 부작용 발생 가능성의 1차적 결정 요인으로 보고, 정밀 차단부터 포괄적 차단까지의 운용 개념 차이를 명확히 구분할 수 있도록 4단계로 정의하였다. 해당 기준은 <표 6-6>에 제시한다.

〈표 6-6〉 전파 방사 부작용 산정 기준 - 정밀성

수준	주파수 정합도	시간 정합도	점수
Level 1 낮음	드론 통신 채널·대역폭까지 정확히 맞춘 1:1 선택적 송출	무력화 시 드론 통신 시간에 맞추어 필요 시에만 송출	1점
Level 2 보통	드론 통신 채널 목록을 알고 해당 채널 전체를 동시에 송출	무력화 시 송출	2~4점
Level 3 높음	드론 통신 채널은 모르지만 대역 내의 특정 영역만 부분적 송출	탐지 시 또는 특정 조건에서 지속 송출	5~8점
Level 4 매우 높음	대역 전체를 포괄적으로 송출	상시 지속 송출	9~10점

또한 불요파 억제력, 무력화 안테나 지향 특성, 전력 세기는 전파 방사가 공간적으로 확산될 수 있는 물리적 조건을 규정하는 요소로, 전파 방사 부작용 발생 가능성의 2차적 결정 요인으로 판단하였다. 이에 따라 이들 요소를 상대적 수준 차이를 반영할 수 있도록 5단계로 구분하였으며, 세부 기준은 <표 6-7>에 제시한다.

〈표 6-7〉 전파 방사 부작용 산정 기준 - 방사 특성

수준	불요파 억제력	전파 방사 각도	전력 세기	점수
Level 1 매우 낮음	우수	단일 방향	저출력	1점
Level 2 낮음	양호	단일 섹터	중저출력	2~4점
Level 3 보통	보통	복수 섹터	중출력	5~6점
Level 4 높음	미흡	광범위	고출력	7~9점
Level 5 매우 높음	취약	전방위	초고출력	10점

다만 불요파 억제력, 전파 방사 각도 전력 세기 등 전파 방사의 방사 특성 요소는 장비 내부 설계, 운용 구성, 설치 환경 및 운용 조건에 따라 실제 전파 확산 특성이 크게 달라질 수 있다. 또한 스퓨리어스(Spurious) 방사량, 방사 패턴, 방사 전력등 세부 성능 지표를 장비 간에 일관되게 비교·산정하는 데 현실적인 한계가 존재한다. 다만 향후 실증 연구 또는 실제 장비 적용 단계에서는 불요 방사량, 안테나 방사 패턴, 송출 전력 수준 등 정량적 지표를 활용한 세부 평가가 필요할 것으로 판단된다.

한편, 전파 방사로 인한 부작용 발생 가능성은 전파 방사의 운용 특성뿐만 아니라, 해당 전파가 수신되는 방송시설의 전파 환경 특성에 따라 달라질 수 있다. 동일한 전파 방사 조건이라 하더라도, 수신 주파수 대역의 전파 전파 특성에 따라 혼신의 발생 범위와 영향 수준에는 차이가 존재한다. 이에 본 연구에서는 전파 방사 부작용 발생 가능성을 보다 현실적으로 반영하기 위해, 전파 방사 특성에 의해 산정된 기술적 영향 점수를 <표 6-8>과 같이 주파수 대역별 전파 간섭 특성으로 보정하였다.

〈표 6-8〉 전파 간섭 특성 계수 기준

주파수 대역	전파 간섭 특성	계수
1 GHz 이하	전파가 회절·반사 특성으로 넓게 확산되어 간섭이 발생하기 쉬운 특성	3점
1 GHz ~ 6 GHz	전파 확산과 직진 특성이 혼재되어 환경에 따라 간섭이 발생할 수 있는 특성	2점
6 GHz 이상	전파의 직진성이 강해 확산이 제한되어 간섭 발생 가능성이 상대적으로 낮은 특성	1점

최종적으로 전파 방사 부작용 발생 가능성 점수는 전파 방사의 정밀성 요소와 물리적 확산 요소를 결합한 기술적 영향 점수를 산정한 후, 이를 전파 간섭 특성으로 보정하여 도출한다. 이를 수식으로 표현하면 다음과 같다.

본 연구에서 전파 방사로 인한 부작용은 전파 간섭과 고출력 전파 방사에 따른 회로 손상 가능성으로 구분할 수 있으나, 후자의 경우 출력 수준, 노출 거리, 장비 내성 등 고려해야 할 정량 변수의 범위가 매우 넓어 본 연구의 분석 범위를 벗어나는 것으로 판단하여 평가 대상에서 제외하였다.

이에 따라 본 연구에서는 전파 방사 부작용을 전파 간섭 영향에 한정하여 평가하였으며, 전파 간섭의 발생 가능성과 영향도에 가장 큰 영향을 미치는 요소로 주파수 정합도와 시간 정합도를 핵심 변수로 설정하였다. 해당 두 요소는 간섭 지속성 및 실질적 서비스 영향에 미치는 기여도가 높다고 판단하여, 다른 간섭 요소 대비 2배의 가중치를 부여하였고, 수식은 다음과 같다.

$$\text{발생가능성}_{\text{전파 간섭}} = \frac{(\text{주파수 정합도} + \text{시간 정합도}) \times 2 + \text{불요파 억제} + \text{전파 방향} + \text{전력 세기}}{7} \times \frac{\text{전파 간섭 특성}}{3}$$

이와 같은 산정 방식은 전파 간섭의 발생 가능성을 동일한 10점 척도 내에서 정규화하여, 이후 영향도와 결합한 위험 수준 도출을 가능하게 한다.

○ 하드킬 부작용 발생 가능성

하드킬 방식의 안티드론 시스템은 드론을 물리적으로 무력화하는 방식으로, 위협 대응 효과는 크지만 요격 과정에서 드론 잔해와 탑재물의 낙하를 수반한다는 특성을 가진다.

이에 따라 본 연구에서는 오조준, 운용 실수, 비정상적인 장비 동작과 같은 사고성 요인은 분석 범위에서 제외하고, 정상적인 운용을 전제로 한 하드킬 시스템의 배치 환경과 통제 가능성만을 고려한다. 하드킬 부작용 발생 가능성 평가는 요격 잔해가 피해로 이어질 수 있는 2차 피해 조건과, 해당 상황을 관리·억제할 수 있는 통제 가능성을 결합하여 산정한다.

먼저 하드킬 부작용 발생 가능성의 기본 조건으로서, 요격 잔해가 피해로 이어질 수 있는 2차 피해 가능성을 평가한다. 본 연구에서 2차 피해 가능성을 다음 두가지 요소로 판별한다.

○ 2차 피해 가능성 평가 요소

- 인적 노출도
- 시설 노출도

인적 노출도는 요격 잔해 낙하 가능 구역 내에 상시 또는 주기적으로 인원이 존재할 가능성을 의미하며, 시설 노출도는 요격 잔해로 인해 기능 저하 또는 물리적 손상이 발생할 수 있는 주요 설비나 구조물이 존재할 가능성을 의미한다. 각 요소는 1~10점 척도로 평가되며, 점수가 높을수록 요격 잔해가 실제 피해로 이어질 수 있는 환경적 조건이 성립할 가능성이 높음을 의미한다. 2차 피해 가능성에 대한 산정 기준은 다음 <표 6-9>과 같다.

〈표 6-9〉 2차 피해 가능성 산정 기준

수준	인적 노출도 기준	시설 노출도 기준	점수
Level 1 매우 낮음	상시 인원 없음 또는 극히 제한적 출입	시설물 없음 또는 기능·운영에 영향이 없는 공간	1점
Level 2 낮음	비상주 인원 또는 간헐적 출입 인원 존재	창고, 보관 공간 등 비운영·비핵심 설비 노출	2점
Level 3 보통	상시 근무 인원은 없으나 주기적 작업 인원 존재	케이블 선로, 전원·신호 경로 등 기능 유지에 필요한 선로 노출	3~5점
Level 4 높음	상시 근무 인원 또는 다수 인원이 지속적으로 존재	핵심 설비 노출 (송수신기, 제어 장비, 안테나 등)	6~10점

본 연구에서는 인적 노출도와 시설 노출도를 동일한 중요도로 간주하여, 두 점수의 평균값을 2차 피해 가능성 점수로 산정한다. 이를 통해 특정 요소에 과도하게 치우치지 않고, 요격 잔해 낙하로 인한 피해 발생 조건을 균형 있게 반영하도록 한다.

한편, 동일한 노출 조건을 갖는 환경이라 하더라도 요격 상황에 대한 통제 가능성에 따라 실제 요격 잔해 낙하로 인한 피해 발생 가능성은 달라질 수 있다. 이에 본 연구에서는 요격 시점, 요격 위치, 요격 고도 및 낙하 구역에 대한 통제 가능성을 하드킬 부작용 발생 가능성 산정의 조정 변수로 적용한다. 통제 가능성은 실시간 운용 숙련도가 아닌, 해당 시설에 구축된 방어 체계의 구성 수준을 기준으로 평가한다.

요격 통제 가능성은 드론 탐지 범위, 탐지 이후 대응까지 소요되는 시간, 요격 타이밍과 위치를 사전에 선택할 수 있는 수준을 종합적으로 고려하여 1~10점 척도로 평가하며, 점수가 높을수록 요격 잔해 낙하를 관리·억제할 수 있는 수준이 높은 것으로 해석한다. 요격 통제 가능성에 대한 산정 기준은 다음 <표 6-10>과 같다.

〈표 6-10〉 요격 통제 가능성 산정 기준

수준	요격 통제 가능성	점수
Level 1 매우 낮음	요격 시점·위치·고도에 대한 선택이 사실상 불가능하며, 낙하 구역을 고려한 운용이 불가능한 상태	1점
Level 2 낮음	드론 접근 인지는 가능하나, 요격 타이밍 및 지점 선택이 제한적이며, 낙하 구역 관리가 곤란한 상태	2~4점
Level 3 중간	요격 타이밍 또는 지점에 대한 제한적 조정이 가능하나, 낙하 범위 통제는 부분적으로만 가능한 상태	5~6점
Level 4 높음	요격 타이밍·지점 선택이 가능하며, 낙하 위험 구역을 회피하는 수준의 운용이 가능한 상태	7~8점
Level 5 매우 높음	요격 시점·지점·고도를 종합적으로 고려한 운용이 가능하며, 의도된 낙하 구역 설정·관리가 가능한 상태	9~10점

이러한 구조를 반영하여, 본 연구에서는 하드킬 부작용 발생 가능성을 다음과 같은 방식으로 산정한다. 먼저 인명 노출도와 시설 노출도의 평균값을 기본 2차 피해 가능성 점수로 산정한 후, 이를 요격 통제 가능성 점수로 조정함으로써 최종 발생 가능성을 도출한다. 이를 수식으로 표현하면 다음과 같다.

$$\text{발생가능성}_{\text{2차 피해}} = \frac{\text{인적 노출도} + \text{시설 노출도}}{2}$$

$$\text{발생가능성}_{\text{하드킬}} = \text{발생가능성}_{\text{2차 피해}} \times ((11 - \text{요격 통제 가능성})/10)^2$$

이와 같은 산정식은 인명 및 시설 노출이 높을수록 발생 가능성이 증가하고, 요격 통제 가능성이 높을수록 발생 가능성이 감소하는 구조를 명확히 반영한다. 또한 산정 결과를 최대 10점 범위로 정규화함으로써, 드론 기반 위협 시나리오 및 소프트킬 운용 부작용 발생 가능성과 동일한 척도 내에서 비교·분석이 가능하도록 한다.

산정된 하드킬 부작용 발생 가능성 점수는 이후 위험 분석 단계에서 영향도(Impact)와 결합하여 위험 수준(Risk Level)을 도출하기 위한 기초 지표로 활용되며, 방송시설 환경에 적합한 하드킬 운용 방식 및 대응체계 도입 여부를 검토하는 데 중요한 판단 근거로 활용된다.

2. 방송시설 위험 수준 산정표

방송시설 위험 수준 산정 결과는 <표 6-11>과 같다. 본 표는 방송시설을 대상으로 식별된 자산과 위협 시나리오를 기준으로, 각 시나리오에 대해 영향도와 발생 가능성을 종합하여 산정한 위험 수준을 정리한 것이다. 산정된 위험 수준은 단일 점수의 나열이 아니라, 서비스 연속성과 시설 안전에 미치는 영향을 반영한 위험 수준으로 구성되었다. 또한 본 연구에서 설정한 위험 허용 기준에 따라 위험 수준을 구간별로 구분하여 시각적으로 표현함으로써, 자산별·위협 유형별 위험 분포와 대응 우선순위를 비교·판단할 수 있도록 하였다.

〈표 6-11〉 방송시설 위험 수준 산정표

시나리오 ID	시나리오 설명	최종 영향도	유형별 발생 가능성						유형별 위험 수준					
			유형 1	유형 2	유형 3	유형 4	유형 5	유형 6	유형 1	유형 2	유형 3	유형 4	유형 5	유형 6
S-A01-01	자폭·폭탄 투하로 주조정실 구조 손상	10.0	3.8	2.4	1.4	0.9	0.6	0.3	38.0	24.0	14.0	9.0	6.0	3.0
S-A01-02	화염병 등의 위협물 투하로 주조정실 화재 발생	8.0	4.8	3.0	1.7	1.2	0.8	0.4	38.4	24.0	13.6	9.6	6.4	3.2
S-A01-03	장착된 총기로 주조정실 인명 피해 발생	7.0	3.0	1.9	1.1	0.8	0.5	0.3	21.0	13.3	7.7	5.6	3.5	2.1
S-A01-04	불법 정찰로 주조정실 위치·구조 노출	2.3	5.8	3.7	2.1	1.4	0.9	0.5	13.3	8.5	4.8	3.2	2.1	1.2
S-A01-05	사이버 공격으로 송출 제어 시스템 침해	4.7	2.5	1.6	0.9	0.6	0.4	0.2	11.8	7.5	4.2	2.8	1.9	0.9
S-A01-06	주조정실 인근 공역 단순 침범으로 업무 혼선	1.7	9.3	5.9	3.3	2.3	1.5	0.8	15.8	10.0	5.6	3.9	2.6	1.4
S-A01-07	주조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	2.0	9.3	5.9	3.3	2.3	1.5	0.8	18.6	11.8	6.6	4.6	3.0	1.6
S-A02-01	자폭·폭탄 투하로 부조정실 구조 손상	9.7	4.0	2.6	1.4	1.0	0.6	0.4	38.8	25.2	13.6	9.7	5.8	3.9
S-A02-02	화염병 등의 위협물 투하로 부조정실 화재 발생	7.7	5.0	3.2	1.8	1.3	0.8	0.5	38.5	24.6	13.9	10.0	6.2	3.9

S-A02-03	장착된 총기로 부조정실 인명 피해 발생	7.0	3.3	2.1	1.1	0.8	0.5	0.3	23.1	14.7	7.7	5.6	3.5	2.1
S-A02-04	불법 정찰로 부조정실 위치·구조 노출	2.3	6.0	3.8	2.0	1.5	0.9	0.6	13.8	8.7	4.6	3.5	2.1	1.4
S-A02-05	사이버 공격으로 방송 제작 및 제어 시스템 침해	4.7	2.5	1.6	0.8	0.6	0.4	0.3	11.8	7.5	3.8	2.8	1.9	1.4
S-A02-06	부조정실 인근 공역 단순 침범으로 업무 혼선	1.7	9.5	6.1	3.4	2.4	1.5	0.9	16.2	10.4	5.8	4.1	2.6	1.5
S-A02-07	부조정실 인근 공역 비행 이후 외벽 충돌로 부수적 피해	2.0	9.5	6.1	3.4	2.4	1.6	0.9	19.0	12.2	6.8	4.8	3.2	1.8
S-A03-01	자폭·폭탄 투하로 연주소 송신 시설 파괴	10.0	6.5	4.2	2.3	1.6	1.0	0.6	65.0	42.0	23.0	16.0	10.0	6.0
S-A03-02	화염병 등의 위협물 투하로 연주소 송신 설비 화재 발생	9.0	7.5	4.8	2.7	1.9	1.2	0.7	67.5	43.2	24.3	17.1	10.8	6.3
S-A03-03	장착된 총기로 연주소 송신 설비 인근의 인명 피해 발생	3.0	3.8	2.4	1.4	0.9	0.6	0.3	11.4	7.2	4.2	2.7	1.8	0.9
S-A03-04	불법 정찰로 연주소 송신 설비 위치·구조 노출	2.3	9.3	5.9	3.3	2.3	1.5	0.8	21.4	13.6	7.6	5.3	3.5	1.8
S-A03-05	사이버 공격으로 송신 시스템 침해	5.7	4.3	2.7	1.5	1.1	0.7	0.4	24.5	15.4	8.6	6.3	4.0	2.3
S-A03-06	연주소 송신 시설 인근 공역 단순 침범으로 업무 혼선	1.7	9.8	6.2	3.5	2.4	1.6	0.9	16.7	10.5	6.0	4.1	2.7	1.5
S-A03-07	연주소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	7.0	9.8	6.2	3.5	2.4	1.6	0.9	68.6	43.4	24.5	16.8	11.2	6.3
S-A03-10	요격 잔해가 연주소 송신 시설에 2차 피해	4.3	-	-	-	-	2.9	0.7	-	-	-	-	12.5	3.0
S-A03-11	요격 후 폭발물이 연주소 송신 시설에 2차 피해	10.0	-	-	-	-	2.9	0.7	-	-	-	-	29.0	7.0
S-A04-01	자폭·폭탄 투하로 연주소 주변 시설 파괴	3.0	6.8	4.3	2.4	1.7	1.1	0.6	20.4	12.9	7.2	5.1	3.3	1.8
S-A04-02	화염병 등의 위협물 투하로 연주소 주변 시설 화재 발생	2.7	8.0	5.1	2.9	2.0	1.3	0.7	21.6	13.8	7.8	5.4	3.5	1.9
S-A04-03	장착된 총기로 연주소 주변 시설 인근의 인명 피해 발생	3.0	5.5	3.5	2.0	1.4	0.9	0.5	16.5	10.5	6.0	4.2	2.7	1.5
S-A04-04	불법 정찰로 연주소 주변 시설 위치·구조 노출	1.7	9.8	6.2	3.5	2.4	1.6	0.9	16.7	10.5	6.0	4.1	2.7	1.5
S-A04-05	사이버 공격으로 주변 시설 민간 네트워크 사이버 침해	1.7	6.0	3.8	2.2	1.5	1.0	0.5	10.2	6.5	3.7	2.6	1.7	0.9
S-A04-06	연주소 주변 시설 인근 공역 단순 침범으로 업무 혼선	1.7	10.0	6.4	3.6	2.5	1.6	0.9	17.0	10.9	6.1	4.3	2.7	1.5
S-A04-07	연주소 주변 시설 인근 공역 비행, 시설 충돌로 부수적 피해	2.0	10.0	6.4	3.6	2.5	1.6	0.9	20.0	12.8	7.2	5.0	3.2	1.8
S-A04-10	요격 잔해가 연주소 주변 시설에 2차 피해	2.7	-	-	-	-	2.2	0.5	-	-	-	-	5.9	1.4
S-A04-11	요격 후 폭발물이 연주소 주변 시설에 2차 피해	10.0	-	-	-	-	2.2	0.5	-	-	-	-	22.0	5.0

S-A05-01	자폭·폭탄 투하로 송·중계소 수신 시설 파괴	10.0	6.5	4.2	2.3	1.6	1.0	0.6	65.0	42.0	23.0	16.0	10.0	6.0
S-A05-02	화염병 등의 위협물 투하로 송·중계소 수신 설비 화재 발생	8.0	7.5	4.8	2.7	1.9	1.2	0.7	60.0	38.4	21.6	15.2	9.6	5.6
S-A05-03	장착된 총기로 송·중계소 수신 설비 인근의 인명 피해 발생	6.0	3.8	2.4	1.4	0.9	0.6	0.3	22.8	14.4	8.4	5.4	3.6	1.8
S-A05-04	불법 정찰로 송·중계소 수신 설비 위치·구조 노출	3.7	9.3	5.9	3.3	2.3	1.5	0.8	34.4	21.8	12.2	8.5	5.6	3.0
S-A05-05	사이버 공격으로 수신 시스템 침해	3.7	4.3	2.7	1.5	1.1	0.7	0.4	15.9	10.0	5.6	4.1	2.6	1.5
S-A05-06	송·중계소 수신 시설 인근 공역 단순 침범으로 업무 혼선	1.7	9.8	6.2	3.5	2.4	1.6	0.9	16.7	10.5	6.0	4.1	2.7	1.5
S-A05-07	송·중계소 수신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	7.0	9.8	6.2	3.5	2.4	1.6	0.9	68.6	43.4	24.5	16.8	11.2	6.3
S-A05-10	요격 잔해가 송·중계소 수신 시설에 2차 피해	3.3	-	-	-	-	2.2	0.5	-	-	-	-	7.3	1.7
S-A05-11	요격 후 폭발물이 송·중계소 수신 시설에 2차 피해	10.0	-	-	-	-	2.2	0.5	-	-	-	-	22.0	5.0
S-A06-01	자폭·폭탄 투하로 송·중계소 송신 시설 파괴	10.0	6.5	4.2	2.3	1.6	1.0	0.6	65.0	42.0	23.0	16.0	10.0	6.0
S-A06-02	화염병 등의 위협물 투하로 송·중계소 송신 설비 화재 발생	8.3	7.5	4.8	2.7	1.9	1.2	0.7	62.3	39.8	22.4	15.8	10.0	5.8
S-A06-03	장착된 총기로 송·중계소 송신 설비 인근의 인명 피해 발생	3.0	3.8	2.4	1.4	0.9	0.6	0.3	11.4	7.2	4.2	2.7	1.8	0.9
S-A06-04	불법 정찰로 송·중계소 송신 설비 위치·구조 노출	3.7	9.3	5.9	3.3	2.3	1.5	0.8	34.4	21.8	12.2	8.5	5.6	3.0
S-A06-05	사이버 공격으로 송신 시스템 침해	3.7	4.3	2.7	1.5	1.1	0.7	0.4	15.9	10.0	5.6	4.1	2.6	1.5
S-A06-06	송·중계소 송신 시설 인근 공역 단순 침범으로 업무 혼선	1.7	9.8	6.2	3.5	2.4	1.6	0.9	16.7	10.5	6.0	4.1	2.7	1.5
S-A06-07	송·중계소 송신 시설 인근 공역 비행, 시설 충돌로 부수적 피해	8.0	9.8	6.2	3.5	2.4	1.6	0.9	78.4	49.6	28.0	19.2	12.8	7.2
S-A06-10	요격 잔해가 송·중계소 송신 시설에 2차 피해	3.3	-	-	-	-	2.2	0.5	-	-	-	-	7.3	1.7
S-A06-11	요격 후 폭발물이 송·중계소 송신 시설에 2차 피해	10.0	-	-	-	-	2.2	0.5	-	-	-	-	22.0	5.0
S-A07-08	AM 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9
S-A08-08	국제 단파 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9
S-A09-08	FM 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9
S-A10-08	DMB 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9
S-A11-08	디지털 TV 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9

S-A12-08	UHD 방송 전파 간섭	2.7	-	-	6.4	2.6	-	8.1	-	-	17.3	7.0	-	21.9
S-A13-08	운용 및 제어 신호 전파 간섭	3.7	-	-	4.3	1.7	-	5.4	-	-	15.9	6.3	-	20.0
S-A14-08	프로그램 중계 링크 전파 간섭	4.7	-	-	4.3	1.7	-	5.4	-	-	20.2	8.0	-	25.4
S-A15-08	TV 이동 중계 링크 전파 간섭	4.7	-	-	4.3	1.7	-	5.4	-	-	20.2	8.0	-	25.4
S-A16-08	방송 고정 중계 링크 전파 간섭	4.7	-	-	2.1	0.9	-	2.7	-	-	9.9	4.2	-	12.7

● 저 자 소 개 ●

이 승 준

- 한림대 정보통신학과 졸업
- 고려대 정보보호학과 박사 수료
- 현 주식회사 본레이크 대표이사

이 영 우

- 세종대 정보보호학과 졸업
- 세종대 정보보호학과 석사
- 현 주식회사 본레이크 전무이사

황 철 민

- 나사렛대 정보통신학과 졸업
- 현 주식회사 본레이크 상무이사

방송통신융합 정책연구 KMCC-2025-41

방송시설 보호를 위한 안티드론시스템 구축 방안 연구

2025년 12월 31일 인쇄
2025년 12월 31일 발행

발행인 방송미디어통신위원회 위원장
발행처 방송미디어통신위원회
경기도 과천시 관문로 47
정부과천청사 2동
TEL: 02-2110-1323
Homepage: www.kmcc.go.kr