JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항행 및 항법

J. Adv. Navig. Technol. 28(4): 442-449, Aug. 2024

UAM 통신, 항법, 감시 및 정보 시스템의 사이버 위협 분석

Cyber Threat Analysis of UAM Communications, Navigation, Surveillance and Information System

김 경 욱* · **윤 형 근**
한화시스템

Kyungwook Kim* · **Hyoung-keun Yoon**
Hanwha Systems, Gyeonggi-do, 13524, Korea

[요약]

본 연구는 도심항공교통(UAM; urban air mobility) 혹은 미래항공교통(AAM; advanced air mobility) 인프라의 통신, 항법, 감시 및 정보 시스템 인프라에 대한 사이버 위협 분석을 위한 포괄적인 프레임워크를 제안하고자 한다. 잠재적인 취약점과 위협 벡터를 검토함으로써 UAM 인프라의 보안과 회복력을 강화하려고 한다. 또한, 다양한 유형의 사이버 위협을 식별하고 분류하며, 이들 위협이 CNSi 시스템에 미치는 영향을 평가하고, 이러한 위협으로 악용될 수 있는 시스템 내의 취약점을 평가하는 상세한 사이버 위협 분석을 수행하고자 한다. 해당 연구는 UAM 시스템의 배치 및 운영에 참여하는 이해관계자들에게 귀중한 통찰을 제공하고, 궁극적으로 도시 공중 교통의 안전하고 효율적인 통합에 기여하는 것을 목적으로 한다.

[Abstract]

In this paper, we aim to propose a comprehensive framework for cyber threat analysis of urban air mobility (UAM) or advanced air mobility (AAM) communications, navigation, surveillance, and information system infrastructure. By examining potential vulnerabilities and threat vectors, we seek to enhance the security and resilience of UAM infrastructure. We conduct a detailed cyber threat analysis to identify and categorize various types of cyber threats, assess their impact on the CNSi systems, and evaluate the vulnerabilities within these systems that may be exploited by such threats. This analysis will provide valuable insights for stakeholders involved in the deployment and operation of UAM systems, ultimately contributing to the safe and efficient integration of urban air transportation.

Key word : Advanced air mobility, Urban air mobility, Cyber-security, Communication, Surveillance.

http://dx.doi.org/10.12673/jant.2024.28.4.442

Received 9 August 2024; **Revised** 27 August 2024
Accepted (Publication) 29 August 2024 (30 August 2024)

***Corresponding Author; Kyungwook Kim**

Tel: ***-****-****

E-mail: kevinkim86@hanwha.com

Ⅰ. 서 론

본 연구는 2028년 상용화 예정인 도심항공교통(UAM; urban air mobility) 혹은 미래항공교통(AAM; advanced air mobility) 인프라의 CNSi[1] 시스템에 대한 사이버 위협을 분석하였다.

CNSi는 통신·항법·감시·정보 시스템의 종합 체계라고 할 수 있으며, 기존의 전통적인 항공 분야에서 널리 사용된다. 다시 말해서 항공 시스템의 인프라 전반으로 설명되는 항공 생태계라고 볼 수 있으며, 추가로 항공교통관리(ATM; air traffic management)를 포함해서 CNS/ATM[2]으로 표현되기도 한다. 이는 항공기와 관제소 간 통신, 시스템과 사용자 간 통신, 항행안전을 위한 항법 및 감시정보 획득, 각 이해관계자 간 데이터 공유 및 교환 체계 등으로 구성된다[1].

이처럼 안전한 UAM 운항 및 관제 있어서 CNSi는 필수적이며, CNS/ATM 인프라를 기반으로 서비스가 제공된다. 다양한 센서와 장비가 인프라 전반에 설치가 될 것이며, 수신되는 데이터를 기반으로 운항 및 관제가 이루어지게 된다. 각각 역할과 임무가 있는 센서들에 대해서는 뒤에서 다루게 될 것이며, 해당 센서의 취약점을 분석하고 발생 가능한 사이버 위협 시나리오를 구성하고자 한다.

결과적으로 본 연구는 UAM 인프라와 서비스에 있어서 CNSi 지상 시스템을 중심적으로 발생 가능한 사이버 위협을 분석하고 이에 대한 대응방안을 마련하기 위해서 작성되었다.

Ⅱ. 연구 배경

2-1 CNS/ATM의 주요 구성요소

미국연방항공국 (FAA; Federal Aviation Administration)는 UAM 인프라를 운영하기 위해서 공역, 운영 유형, 규정 및 절차가 수립되어야 한다고 설명하였으며, 분야별 구성요소로는 항공교통관제를 위한 분리 기준, 항공교통 흐름관리, 그리고 CNS 기반의 인프라가 구축되어야 한다고 설명한다[2].

국내에서도 UAM 상용화에 앞서 각종 국책과제와 실증사업이 활발히 진행되고 있으며, 대표적으로 국토교통부 UAM Team Korea에서는 UAM 인프라에 있어서 CNSi의 각 요소별 역할을 정의하였다[3]. 표 1을 통해서 K-UAM 운용개념서 기반의 CNSi 시스템의 역할을 확인할 수 있다.

또한, 국토교통과학기술진흥원의 “저밀도 도심항공모빌리티 교통관리 CNSi 획득 활용 체계 신뢰성 검증 기술 개발” 과제는 2022년부터 진행되고 있으며, 본 연구와 가장 밀접한 연관성이 있다.

1) CNSi(Communication Navigation Surveillance and information): 통신·항법·감시·정보 시스템

2) CNS/ATM(Communication Navigation Surveillance/Air Traffic Management): 국제표준의 차세대 항행시스템

표 1. K-UAM 통신 항법 감시 정보 시스템
Table. 1. K-UAM CNSi system.

Classification	Roles and Responsibility
C (Communication)	Stable information and communication services must be provided in the UAM corridor by using commercial mobile communication.
N (Navigation)	GNSS and SBAS must be used on the route to apply performance-based navigation.
S (Surveillance)	Surveillance data and UAM aircraft operation information must be obtained by using commercial mobile communication.
i (Information)	The status information of the aircraft components related to flight safety must be delivered to the UAM operator.

세부적으로 기존 민간 항공 분야에는 다양한 CNS/ATM 장비들이 존재한다. 각 장비들의 목적성에 따라서 주파수로 구분되며, 항행안전에 있어서 1950년대부터 전통적으로 사용되었다.

대표적으로 항공기의 위치와 방향을 추적하고 감시하기 위한 주 감시레이다(PSR; primary surveillance radar)와 2차 감시레이다(SSR; secondary surveillance radar)가 있다. 또한, 운항중인 항공기의 ID, 위치, 고도, 속도 등 다양한 비행 정보를 항공기에서 지상으로 전송해 주는 시스템인 ADS-B(automatic dependent surveillance-broadcast)가 있다.

조종사와 ATC 간 음성통신을 위해서 사용되는 VHF(very high frequency)가 있으며, 이는 초단파 음성통신을 기반으로 필요한 정보를 공유하며 비행한다. CPDLC(controller pilot data link communications)도 필수적이며, VHF 장애 시 유용하게 사용되는 데이터링크 통신 체계다. 음성통신 외에도 전문으로 조종사와 ATC 간 통신을 할 수 있는 수단으로 사용된다. 또 다른 통신수단으로 DSCN(digital satellite communication network)이 있으며, 항공기의 위성통신망에 해당한다.

항공기의 이착륙 단계에서 항행안전을 지원하는 시설로 DME(distance measuring equipment)가 있으며 기체와 활주로 사이의 거리를 측정하기 위한 거리측정장비다, 또한, 기체의 LoS(line of sight)를 지원하기 위한 초단파 전방향 무선표지인 VOR(VHF omni-directional range)도 있다. 추가로 계기착륙을 지원하는 ILS(instrument landing system)가 있으며, 이는 기체의 안전한 착륙을 지원하기 위한 항행안전시설이라고 볼 수 있다.

2-2 UAM 인프라의 CNS/ATM 인프라 분석

본격적인 항공교통관리는 1950년대 FAA의 NAS[3]가 등장하면서 시작되었으며, 여기에 항행안전을 위한 감시 레이다 등 다양한 통신·항법·감시 센서들이 표준으로 등장하게 된다[4].

3) NAS(National Air Space): 항법시설, 공항, 정보, 시스템을 포함하는 미국의 영공 시스템

본 연구에서 집중적으로 다룰 CNS/ATM은 1980년대 항공 교통량과 연결성 증가로 인하여 현대화된 시스템의 필요성에 의해서 등장하게 되었으며, 이는 NAS를 기반으로 고도화된 시스템이라고 볼 수 있으며, NextGen[4]으로도 불리게 되었다. 다만, 약 50년 전 이와 같은 항법 시스템, air-to-air 정보 교환, air-to-ground 정보 교환, 비행 제어, 승객 엔터테인먼트 및 안전 등 수많은 항공 관련 통신 시스템이 사용되었으나, 해당 시스템 일부는 사이버보안을 염두에 두지 않고 만들어졌다[5].

UAM 인프라의 전반적인 CNS/ATM 프레임워크는 그림1을 통해서 확인할 수 있다. 지상부터 우주까지 다양한 시스템과 센서가 존재하며, 지상에서 UAM 운항 및 관제를 위한 PSU[5], UAMO[6], VPO[7], SDSP[8], 그리고 공공 업무를 담당하는 기타 이해관계자 등으로 구성되어 있으며, 상호 간 데이터 교환은 SWIM[9]을 통해서 이루어진다. 여기서 SWIM이 CNSi에 있어서 information을 뜻하는 "i"를 담당하게 된다. 각종 항법 및 감시 장비로는 ADS-B[10], 탐지레이다, 영상감시시스템 등이 존재한다. 해당 인프라를 기반으로 UAM을 조종하는 PIC[11]가 있을 것이며, air-to-air, air-to-ground 통신이 발생하게 된다. 여기에 초연결을 실현하기 위한 저궤도 위성(LEO; low-earth orbit) 통신까지 갖춰지게 되면 UAM 인프라가 완성되게 된다. 결과적으로 크게 Ground, Air, Space로 구분될 수 있으며, 각 구간의 기술 요소들은 상호 간 연결되어 있으며, UAM의 안전한 비행을 보장하기 위한 기본적인 구성이라고 볼 수 있다.

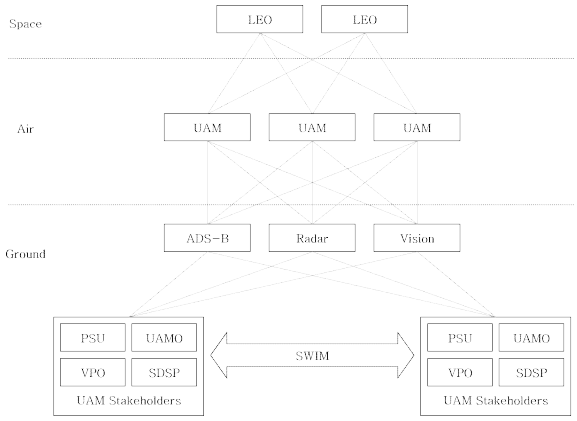

그림 1. UAM 인프라의 전반적인 CNS/ATM 프레임워크
Fig. 1. Overall CNS/ATM framework of UAM infrastructure.

4) NextGen(Next Generation Air Transportation System): 친환경, 효율, 안전을 표방한 차세대 항공운송시스템을 구축하려는 미국의 국가항공 장기계획(2006~2025년)
5) PSU(Provider of Services for UAM): UAM 교통관리서비스 제공자
6) UAMO(UAM Operator): UAM 운항자 혹은 운항사
7) VPO(Vertiport Operator): 버티포트 혹은 공항 운영자
8) SDSP(Supplemental Data Service Providers): 운항지원정보 제공자
9) SWIM(System Wide Information Management): 각종 시스템 전반에 걸친 정보를 이해관계자 간 공유하기 위한 데이터 교환 모델
10) ADS-B(Automatic Dependent Surveillance-Broadcast): 항공기의 감시 정보(항공기 식별 부호, 위치, 속도, 방향 등)를 1초 단위로 지상의 ATC 시스템과 다른 항공기에 방송
11) PIC(Pilot In Command): UAM 조종사

해당 인프라는 UAM의 운항 및 관제를 위해서 기본적으로 갖추어야 할 구성요소이며, 상용화가 되기 전까지 지속적인 연구와 실증을 통해서 정의 될 것으로 예상된다. 또한, 그 과정에서 UAM을 위한 표준화도 진행될 것이며, 기존 항공분야를 구성요소를 적극 반영 및 활용하여 지역별로 적합한 인프라가 구축될 것으로 보인다.

Ⅲ. UAM 통신, 항법, 감시 및 정보 시스템의 사이버 위협 분석

3-1 사이버 위협의 종류

인터넷의 등장과 연결성이 커짐에도 불구하고 항공 시스템을 전통적인 방식 그대로 유지하는 경향이 컸다. 타 산업군에서는 빅데이터와 AI가 집약되어 생산성을 극대화하는 움직임이 많으나 항공분야는 승객의 안전을 고려하여 최소한의 변화만 추구한다. 신기술을 바탕으로 효율성을 극대화하는 것 보다 기존 체계를 유지하면서 안정성을 보장하는 것을 더 중요시했다.

이와 같은 방향성이 최선의 선택일 수 있겠으나 사전에 인지하지 못하는 잠재적인 취약점과 사이버 위협은 존재한다. 따라서 해당 시스템에 대한 잠재적 사이버 위협을 고려하여 인프라를 구축해야 하며, 그러기 위해서는 사이버 위협의 구조를 이해해야 한다.

해당 인프라에서 발생할 수 있는 사이버 위협은 크게 3가지로 구분될 수 있다. 정보보안의 3요소인 가용성(availability), 무결성(integrity), 기밀성(confidentiality)을 바탕으로 사이버 위협에 대한 개략적인 구조도를 그림2와 같이 구성하였다.

사이버 위협에 있어서 궁극적인 목표는 예상하지 못하는 시점에 불법적인 방법을 동원하여 악의적인 영향을 미치는 것이다. 악의적인 영향은 목표 시스템과 서비스가 이용 불가하도록

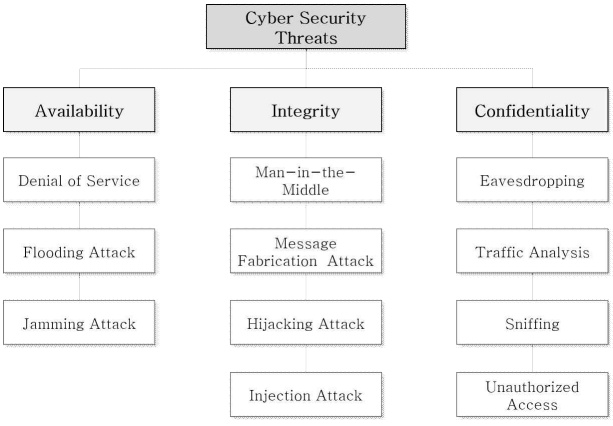

그림 2. 사이버 위협 개략 구조도
Fig. 2. Cyber threat architecture overview.

방해하는 가용성 측면의 공격이 있을 수 있으며, 대표적으로 과도한 트래픽을 발생시켜 서비스를 마비시키는 분산 서비스 거부 공격인 DoS(denial of service) 혹은 다수의 PC를 감염시켜 공격에 동원하는 DDoS(distributed denial of service) 공격이 있다. 이를 비롯하여 각종 트래픽에 영향을 주는 플로딩 공격과 재밍 공격을 통해서 서비스를 마비시키는 공격을 발생시킬 수 있다.

무결성 측면에서는 해당 시스템 내에서 상호 교환되는 데이터와 자료를 변조하는 공격이 이루어질 수 있다. 무결성을 깨트리기 위한 침해사고는 목표 시스템과 서비스에 공격자가 직접적으로 관여하여 영향을 행사할 수 있다는 것을 의미하기 때문에 매우 심각한 사이버 위협으로 간주한다. 중간자 공격을 기반하여 메시지 변조 공격, 하이재킹 공격과 인젝션 공격이 이루어진다.

시스템에 직접적인 영향을 행사하는 무결성 공격과 다르게 기밀성을 침해하는 공격은 시스템과 서비스에 직접적인 영향을 주지는 않으면서 몰래 정보를 획득하는 공격 기법으로 구성되어 있다. 일반적으로 감청, 트래픽 분석, 스니핑 등에 해당한다.

3-2 분석 대상 CNSi 시스템

본 연구는 UAM 인프라가 구축되고 상용화가 되기 이전에 CNSi 시스템의 사이버 위협을 사전에 분석하여 향후 발생 가능한 위협에 대응하기 위한 목적을 가진다.

최근 유럽연합 네트워크 및 정보 보안 기구 (ENISA; European Union Agency for Cybersecurity)의 보고서에 따르면, 전 세계 항공 부문은 사이버 공격과 ICT 종속성 중단을 포함한 정보 보안 사고가 급격하게 증가하고 있다고 설명한다[6].

연구배경에서 다뤘던 기존 항공분야의 CNS/ATM의 주요 구성요소 중 UAM 인프라에 적합한 구성요소를 그림3과 같이 정리해 볼 수 있다. 앞서 2장에서 설명한 CNS/ATM 시스템이 좌측에 모두 나열되어 있으며, 활주로를 이용하여 이착륙하는 항공기를 관제하기 위한 센서들로 구성되어 있다. 우측에는 UAM 혹은 AAM 인프라에 초기적으로 필요한 센서들로 구성되어 있으며, 일부 간소화가 된 모습을 볼 수 있다.

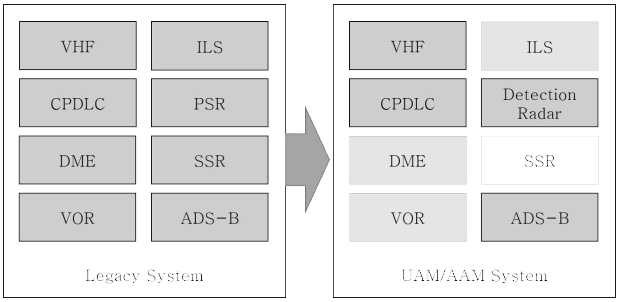

그림 3. UAM 인프라의 CNS/ATM 시스템
Fig. 3. CNS/ATM system for UAM infrastructure.

VHF, CPDLC의 경우 기존 항공기와 더불어 여전히 사용될 통신 시스템일 것으로 예상된다. 현재 개발이 진행되고 있는 UAM 기체의 경우 기체 설계 단계에서부터 해당 항전시스템을 포함하여 개발하고 있으며, 현재 감항인증을 앞둔 상황에서 기존의 전통적인 시스템을 그대로 차용하여 적용하는 것이 안정성 측면에서도 검증이 되어 적합할 것으로 보인다.

ADS-B도 기존 항공기와 마찬가지로 트랜스폰더가 장착되어 기체와 지상 간 감시가 이루어질 것으로 보이며, 가장 필수적인 감시 시스템으로 활용될 것이다.

기존 레이다의 경우 PSR과 SSR로 구분되어 있었으나, UAM을 감시하기 위해서는 해당 고도와 범위에 적합한 탐지레이다를 개발하는 것이 가장 적합할 것이다.

SSR의 경우 4~5초마다 관제 대상인 항공기의 위치, 거리, 고도 및 상태 정보를 지상으로 보내주게 된다. 반면 ADS-B의 경우 SSR에 제공하는 데이터와 유사하지만, 전송하는 속도를 비교했을 때 ADS-B는 1초마다 정보를 방송한다[7].

따라서 위치 정보만 제공하는 PSR의 성능을 보완하기 위해서 개발되었으나, 1시간 미만의 비행 거리와 1,000~2,000 ft 고도를 비행하는 UAM의 경우 ADS-B를 통해서 확보되는 비행 데이터와 탐지레이다의 감시 데이터를 바탕으로 관제해도 무리가 없을 것으로 예상한다.

결국 하나의 UAM 탐지레이다 하드웨어 구성이 기존의 PSR과 SSR 역할을 하게 될 것이며, UAM 회랑 내 비행하는 기체와 비협력적 대상을 감시하거나 버티포트 이착륙 단계 시 기체의 감시 및 관제를 지원하기 위해서 사용될 것이다. 이는 목적에 따라서 구분될 수 있으며, 다양한 방면으로 활용도가 높을 것으로 예상한다.

UAM은 출도착 단계에서는 헬기와 유사한 형태의 회전익 모형으로 비행하며, 순항단계에서는 기존 항공기와 동일한 고정익 모형으로 비행하게 된다. 물론 기체의 형상와 설계에 따라서 상이할 수 있으나, 감항인증과 형식증명이 가장 빠르게 진행될 모델의 경우 회전익과 고정익 사이를 천이하는 과정이 포함되어 있다. 따라서 DME, VOR, ILS 등 기체와 활주로 사이의 거리를 측정하고 안전한 착륙을 지원하는 항행안전시설은 UAM 기동에 적합하게 개량하여 구축되어야 한다.

결과적으로 아직 UAM 혹은 AAM 인프라에 대한 항행안전시설 표준이 없는 상태이며, 전 세계적으로 각종 연구과제 및 실증사업이 진행되고 있다. 또한 분과별 워킹그룹을 추진하고 있으며, 이를 바탕으로 세부적인 절차와 표준 등을 정의해 나가고 있는 상황으로 시장을 형성하기 위해서 초기적인 활동이 진행되고 있다. 대표적으로 국내에는 K-UAM 드림팀이 관련된 연구과제와 실증사업을 추진하고 있다[8].

이에 대한 UAM 인프라 실증 구조도는 그림 4와 같이 확인할 수 있다.

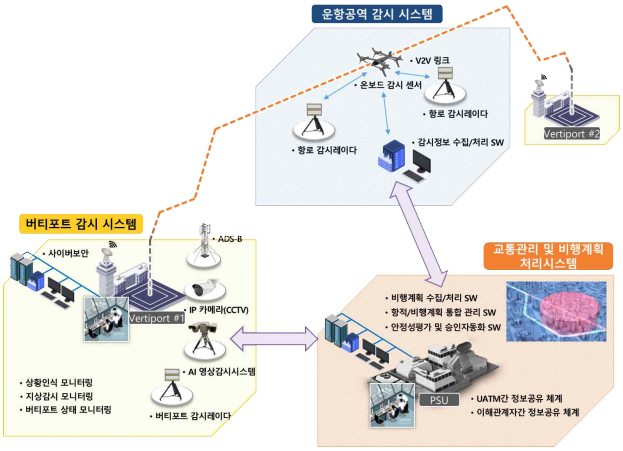

그림 4. UAM 인프라 예상 구조도
Fig. 4. Expected structure of UAM infrastructure.

3-3 사이버 위협 영향을 받는 CNSi 시스템 분석

3-1장에서 설명한 사이버 위협의 종류를 3-2장의 분석 대상 CNSi 시스템을 결합하여 사이버 위협 영향을 받는 CNSi 시스템을 분석하였다. 현재 진행 중인 연구과제와 실증사업을 바탕으로 예상되는 UAM 인프라의 구조를 기반으로 발생할 수 있는 사이버 위협을 정보보안의 3요소로 분류하고 이에 영향을 받는 시스템을 분석하였다.

가용성, 무결성, 기밀성은 모두 중요하겠으나 이에 대한 심각도 혹은 침해를 받지 말아야 하는 우선순위는 각 인프라 환경마다 차이가 있을 수 있다. 예를 들어 특정 분야에 연구개발을 진행하는 연구소의 경우 가장 높은 우선순위는 기밀성이 될 것이다. 반면 IT서비스를 제공하는 데이터센터의 경우 가용성이 가장 치명적인 약점이 될 수 있다.

이처럼 UAM 인프라에서는 시스템에 영향을 직접 주는 가용성과 무결성 공격이 심각도가 높을 수 있다. 이와 같은 위협은 테러에 해당하며, 항행안전에 매우 큰 위협이 될 수 있다. 또한, 상황의 심각도에 따라 인명피해까지 이어질 수 있어 가용성과 무결성 공격에 주의가 필요하다. 다만, 가용성과 무결성 공격을 진행하기 위해서 감청, 트래픽 분석, 스니핑 등 기밀성 관련 공격이 사전에 이루어질 수 있다는 점에서 정보보안의 3요소 모두 선제적으로 적용되어야 한다.

따라서 정보보안의 3요소를 모두 고려하여 UAM 인프라에 대입하여 앞으로 미래에 발생할 수 있는 사이버 위협을 구분해 볼 수 있다. 그러기 위해서 CNSi 시스템별로 정보보안의 3요소를 정리하여 요소별로 영향을 받는 시스템을 표 2를 통해서 확인할 수 있다.

CNSi의 통신 분야는 VHF와 CPDLC가 있겠으며, 이에 대한 위협은 다음과 같이 정리될 수 있다.

표 2. CNSi 시스템의 보안 요소 및 영향을 받는 시스템
Table 2. Security elements and affected system of CNSi system.

Classification	Security Elements	Affected System
Communication Threats	Availability	VHF, CPDLC frequency jamming, CPDLC message flooding
	Integrity	VHF, CPDLC frequency modulation
	Confidentiality	VHF, CPDLC interception, sniffing
Navigation Threats	Availability	ILS jamming
	Integrity	VOR, DME signal interception
	Confidentiality	N/A
Surveillance Threats	Availability	Radar, ADS-B jamming, data flooding
	Integrity	ADS-B data tampering
	Confidentiality	Radar interception, ADS-B eavesdropping
Information Threats	Availability	SWIM(System Wide Information Management)
	Integrity	
	Confidentiality	

우선 VHF의 경우 아날로그 신호 특성상 가시거리 통신에 사용되는 것이 보통이다. 이는 사용 도중에 산악이나 고층 건물 등 차폐물이 있으면 크게 감쇄하게 되며, 통신에 어려움이 발생하게 된다. 이를 보완하기 위해서 등장한 것이 CPDLC이며, 음성 통신 대신 전문 메시지를 지상 기체 간 상호 교환할 수 있는 데이터 링크 통신 기술로 사용된다. 이는 VHF 장애 시 유용하게 사용된다.

다만, CPDLC도 취약점 존재하며, 해당 시스템에는 별도 인증이나 기밀성을 보장할 만한 장치가 없다. 따라서 중복되는 메시지나 지연 또는 누락된 CPDLC 통신이 발생할 수 있으므로 이에 대한 보안이 필요하다. 이는 VHF 통신도 가용성, 무결성, 기밀성 측면에서 동일하게 적용받을 수 있다.

공격자는 CPDLC 수신기를 방해함으로써 채널 용량을 줄여 서비스에 대한 액세스를 차단할 수 있다. 이는 CPDLC 수신 당사자에게 메시지가 도달하는 것을 불가능하게 만들기 위해서 해당 채널에 과도한 노이즈를 채워서 보내게 된다. 만약 폐쇄회로 네트워크에 연결된 모든 사용자는 해당 공격의 영향을 받을 수 있다[9].

해당 이슈를 해결하기 위해서는 지상 수신국의 네트워크 상태를 점검해야 할 것이며, 인증되지 않은 사용자는 차단해야 할 것이다. 또한, 암호화된 소켓 통신을 사용하도록 조치를 해 데이터 무결성을 확보해야 한다.

VHF, CPDLC에 대한 공격 기법은 표3을 통해서 확인할 수 있다.

표 3. VHF, CPDLC에 대한 공격 기법

Table 3. Attack techniques on VHF, CPDLC.

CNSi	Security Elements	Attack Techniques
VHF CPDLC (C)	Availability	frequency jamming, message flooding
	Integrity	frequency modulation
	Confidentiality	interception, sniffing

표 4. VOR, DME, ILS에 대한 공격 기법
Table 4. Attack techniques on VOR, DME, ILS

CNSi	Security Elements	Attack Techniques
VOR DME ILS (N)	Availability	jamming
	Integrity	signal interception
	Confidentiality	N/A

CNSi의 항법 분야는 VOR, DME, ILS와 관련 있겠으며, 이에 대한 위협은 다음과 같이 정리될 수 있다. 단, 본 연구에서는 UAM 인프라 기준 항법과 관련된 기술 요소가 미정인 부분이 있어서 기존 항공분야를 기준으로 명시하였다.

가용성을 침해하는 가장 큰 요소로 재밍이 있으며, 이는 GPS 신호를 방해하게 되면 일어날 수 있다[10].

VOR과 DME에 대한 취약점은 주파수 기반 소프트웨어 정의 라디오 공격이 있을 수 있으며, 주파수 조작을 통한 도청 및 이착륙 방해가 발생할 수 있다. 이를 보완하기 위해서는 암호화 통신을 구축하여 무결성을 확보하는 것이 중요하다.

VOR, DME, ILS에 대한 공격 기법은 표4를 통해서 확인할 수 있다.

CNSi의 감시 분야는 탐지레이다와 ADS-B가 있겠으며, 이에 대한 위협은 다음과 같이 정리될 수 있다.

우선 탐지레이다의 경우 기존 항공분야의 1차 감시레이다인 PSR은 원칙적으로 신호 기반 탐지 접근 방식으로 작동하여 메시지 주입은 불가능하다. 반면에 PSR 작동에 있어서 방해하는 것은 가능하다[11].

따라서 UAM 인프라에서 사용될 수 있는 탐지레이다의 경우 이와 유사하게 무결성에 이슈는 없을 수 있으나 가용성이 침해받을 수 있다. 가장 대표적인 공격 기법으로 재밍 혹은 플로딩 공격이 있을 수 있으며, 이는 지상의 관제센터에서 관제 대상인 UAM의 항적을 확보하거나 비협력적 대상을 식별하는 데 어려움이 있을 수 있다.

추가로 기밀성 측면에서는 발생하는 레이다 신호를 중간에서 가로채는 행위가 발생할 수 있다. 이는 감시 데이터를 수신하여 처리하는 장치에 대한 침해가 있을 때 발생할 수 있으며, 해당 자산에 대한 주기적인 점검이 요구된다.

탐지레이다에 대한 공격 기법은 표5를 통해서 확인할 수 있다.

표 5. Radar에 대한 공격 기법
Table 5. Attack techniques on radar.

CNSi	Security Elements	Attack Techniques
Radar (S)	Availability	jamming, data flooding
	Integrity	N/A
	Confidentiality	interception

ADS-B의 경우 가장 기본적이며, 필수적인 감시 시스템으로 UAM의 위치를 식별하고 필요한 비행 정보를 수신해야 한다. UAM에서 발신되는 데이터가 수신자한테 무결한 상태로 지연없이 전달 되어야 하며, 이 과정에서 발생할 수 있는 사이버 위협은 다수 존재한다.

가용성 측면에서는 ADS-B 메시지와 서비스가 정확하게 전송되지 않고 중간에 중단이 된다던가 너무 많은 양의 데이터가 누적되어 전송되게 되면 심각한 문제를 초래할 수 있다. 예를 들어 공격자는 ADS-B 지상국을 쉽게 방해하고 서비스 거부 공격을 수행할 수 있으며, 세부적으로는 재밍 혹은 플로딩 공격으로 분류될 수 있다[12]. 이는 UAM 기체 내 ADS-B 트랜스폰더를 공격하여 종단에서 발생할 수 있는 위협으로 볼 수 있다.

무결성 측면에서는 ADS-B 메시지가 전송 중에 변경되거나 수정되어서는 안 된다. 결과적으로 메시지를 삭제시키거나 수정하는 공격은 데이터 무결성에 반하는 것이므로 데이터 변조에 주의해야 한다. 이는 UAM 기체 내 ADS-B 트랜스폰더 종단에서 발생하는 위협보다는 중간에서 데이터를 가로채는 행위를 통해서 발생할 수 있다.

기밀성 측면에서는 한계가 있을 수 있다. 비행 중인 기체가 ADS-B를 방송하고 있고 ADS-B 수신기가 지상에 있다면 해당 기체를 모니터링하는 것은 어려운 일이 아니다. 다만 원칙적으로 허가된 사용자와 기관에서만 사용해야 할 것이며, 이를 악의적인 목적으로 도청해서는 안 된다.

ADS-B에 대한 공격 기법은 표6을 통해서 확인할 수 있다.

마지막으로 SWIM의 경우 FIMS[12]와 연결되며, UAM 인프라에 존재하는 모든 이해관계자들간 필요한 정보를 주고받는다. 지상 인프라 관점에서 사이버보안을 대응하는 방안 마련이

표 6. ADS-B에 대한 공격 기법
Table 6. Attack techniques on ADS-B.

CNSi	Security Elements	Attack Techniques
ADS-B (S)	Availability	jamming, data flooding
	Integrity	data tampering
	Confidentiality	eavesdropping

12) FIMS(Flight Information Management System): 조종사국가 비행정보 관리 시스템

필요하며, 이는 TCP/IP 기반의 네트워크를 중심적으로 분석이 이루어져야 한다.

Ⅳ. 결 론

본 연구는 UAM 인프라에 있어서 통신 분야의 VHF, CPDLC를 비롯하여, 항법 분야의 VOR, DME, ILS와 감시 분야의 탐지레이다와 ADS-B에 대한 사이버 위협을 분석해 보았다. 또한, 향후 UAM 상용화 단계에서 안전성과 안정성이 확보될 수 있도록 사이버 위협을 분석하는 데 의의를 두었다.

따라서 UAM 인프라에 예상되는 다양한 CNSi 장비들에 대한 사이버보안 취약점을 다뤘다. 다만, 각 센서마다 세분화된 분석이 진행되지는 않았으며, 구체적인 대응방안 마련은 향후 연구에서 진행되어야 할 것이다.

그러기 위해서는 각 센서들에 대한 보안성 테스트 및 취약점 진단을 진행해야 하며, 깊이 있는 분석이 진행되어야 한다. 그 결과를 바탕으로 UAM 인프라에 적합한 전용의 장비를 개발하고 고도화해 나가야 할 것이다.

전 세계적으로 아직 UAM 혹은 AAM 인프라에 대한 항행안전시설 표준이 없는 상태이며, 단계적으로 정의해 나가야 할 것이다. 그 과정에 있어서 국가기관 주관의 관련된 국책과제, 실증사업, 워킹그룹 활동을 바탕으로 활발히 진행되고 있다.

결과적으로 UAM 인프라에 있어서 CNSi는 상용화 이전에 표준으로 자리 잡아야 할 기반 기술이자 생명과 직결되는 항행안전시설이다. 따라서 드론, 무인기가 아닌 UAM 혹은 AAM으로 인증받은 기체를 도입하여 CNSi 환경을 실증하고 그 결과를 바탕으로 발전시켜 나갈 필요가 있다.

향후 UAM 혹은 AAM 산업이 발전함에 따라 시장이 개화되고 사회적 수용성이 높아질 것으로 예상되며, 신기술이 집약된 새로운 항전시스템이 개발될 수 있을 것이다. 그 이전까지는 현행과 같이 항행안전시스템이 최대한 유지가 될 것이며, 안정화에 우선순위를 둘 것으로 예상된다. 또한, 안정성을 보장하기 위해서는 연구개발 과정에서 사이버보안을 필수적으로 고려하여 진행되어야 할 것이다.

Acknowledgments

본 연구는 2022년~2024년 국토교통부/국토교통과학기술진흥원의 지원으로 수행 중인 과제(과제명 : 저밀도 도심항공모빌리티(UAM) 교통관리용 CNSi 획득·활용체계 신뢰성 검증 기술 개발, 과제번호 : RS-2022-00143625)의 연구 결과이며, 관계부처의 지원에 감사드립니다.

References

[1] G. Dave, G. Choudhary, V. Sihag, I. You, and K. -K. R. Choo, “Cyber security challenges in aviation communication, navigation, and surveillance,” *Computers & Security*, Vol. 102516, pp. 6, Jan. 2022. DOI: 10.1016/j.cose.2021.102516.

[2] Federal Aviation Administration, *UAM concept of operations v2.0*, Federal Aviation Administration Report, pp. 3, 2023. Retrieved from https://www.faa.gov/urban_air_mobility.

[3] Ministry of Land, Infrastructure and Transport UAM Team Korea (UTK), *K-UAM operation concept 1.0*, pp. 33-34, 2024. Retrieved from https://www.molit.go.kr/urban_air_mobility.

[4] Government Accountability Office, *FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen*, Government Accountability Office Report, pp. 1-45, 2023. Retrieved from https://www.gao.gov/products/gao-23-123.

[5] J. C. Haass, S. L. Carter, and R. M. Brooks, *A framework for aviation cybersecurity*, 1st ed. Cambridge, MA: MIT Press, 2018.

[6] European Union Agency for Network and Information Security, *Securing Smart Airports*, 1st ed. Brussels, *Belgium*: European Union Agency for Network and Information Security, p. 78, Dec. 2016.

[7] D. McCallie, J. Butts, and R. Mills, “Security analysis of the ADS-B implementation in the next generation air transportation system,” *International Journal of Critical Infrastructure Protection*, Vol. 4, No. 2, pp. 78–87, Jun. 2011. DOI: 10.1016/j.ijcip.2011.05.002.

[8] Hanwha, K-UAM Dream Team, Full-scale launch of UAM demonstration project to open the sky [Internet], Available: https://www.hanwha.co.kr/newsroom/media_center/news/news_view.do?seq=8217.

[9] A. Gurtov, T. Polishchuk, and M. Wernberg, “Controller–pilot data link communication security,” *Sensors*, Vol. 18, Article No: 1636, pp. 5, May 2018. DOI: 10.3390/s18051636.

[10] H. Sathaye, D. Schepers, A. Ranganathan, and G. Noubir, “Wireless attacks on aircraft landing systems,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, San Francisco: CA, pp. 295–297, Jun. 2019. DOI: 10.1145/3317549.3317583.

[11] G. Dave, G. Choudhary, V. Sihag, I. You, and K. -K. R. Choo, “Cyber security challenges in aviation communication, navigation, and surveillance,” *Computers & Security*, Vol. 102516, pp. 6, Jan. 2022. DOI: 10.1016/j.cose.2021.102516.

[12] M. R. Manesh and N. Kaabouch, “Analysis of vulnerabilities,

attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast system," *International Journal of Critical Infrastructure Protection*, Vol. 19, pp. 7-8, Sep. 2019. DOI: 10.1016/j.ijcip.2017.10.002.

김 경 욱 (Kyungwook Kim)
2023년 2월: 성균관대학교 기술경영학과 (이학 석사)
2013년 8월~2017년 7월: 안랩
2017년 8월~현재: 한화시스템 전문연구원
※관심분야 : UAM/AAM, 사이버보안, 항법, 감시, 정보, 인프라, 네트워크

윤 형 근 (Hyoung-keun Yoon)
2012년 2월: 아주대학교 대학원 유비쿼터스시스템/C4I (이학석사)
1996년 3월~2009년 7월: 국방부
2009년 8월~현재: 한화시스템 수석연구원
※관심분야 : UAM/AAM, 항공정보공유체계, 통합관제체계, 체계통합