2025년 항공보안공모전

UAM 상용화에 따른 사이버 위협 분석 및 대응방안

한서대학교 항공보안학과
김병진, 오재원, 김지영

CONTENTS

주제 선정 배경

도시화와 교통 혼잡 증가, 기술 발전, 친환경 교통 수단 개발 등으로 UAM이 개발되어 상용화됨에 따라 **사이버 보안 위해 요소**로부터 **UAM의 안전한 운항**을 위하여 보안을 지키기 위해 주제를 선정

UAM과 사이버 보안의 연관성

UAM은 자율 비행 드론, 전기 수직 이착륙 항공기(eVTOL), 항공 교통 관리(ATM) 시스템 등 **다양한 디지털 및 통신 기술에 기반한 시스템**이기 때문에 사이버 보안이 UAM환경에서 매우 중요한 요소로 작용

01

UAM 개요

UAM(Urban Air Mobility)

UAM: 전기 수직 이착륙 항공기(eVTOL)을 활용하여 사람과 화물을 운송하는 도시교통체계

국내 계획: 2025년 상용화 목표

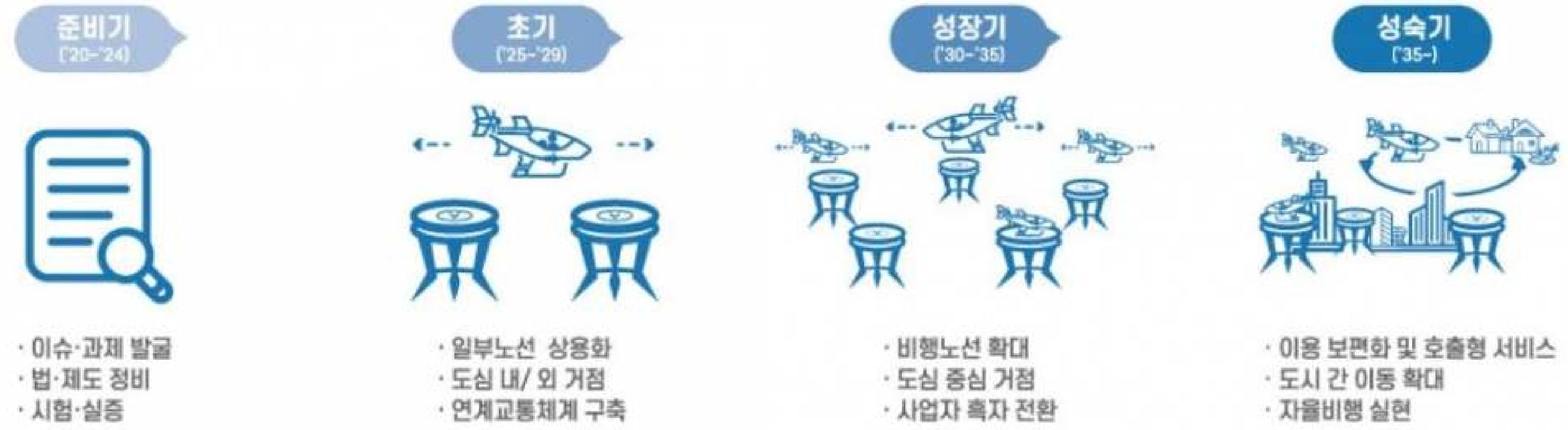
인프라: 버티포트(Vertiport), 관제 시스템 등

UAM은 장기적으로 높은 시장성을 지니고 있음

※버티포트(Vertiport): UAM이 이륙/착륙을 하고 또한 정비 및 충전을 할 수 있는 일종의 정거장

UAM 국내 현황

K-UAM 로드맵

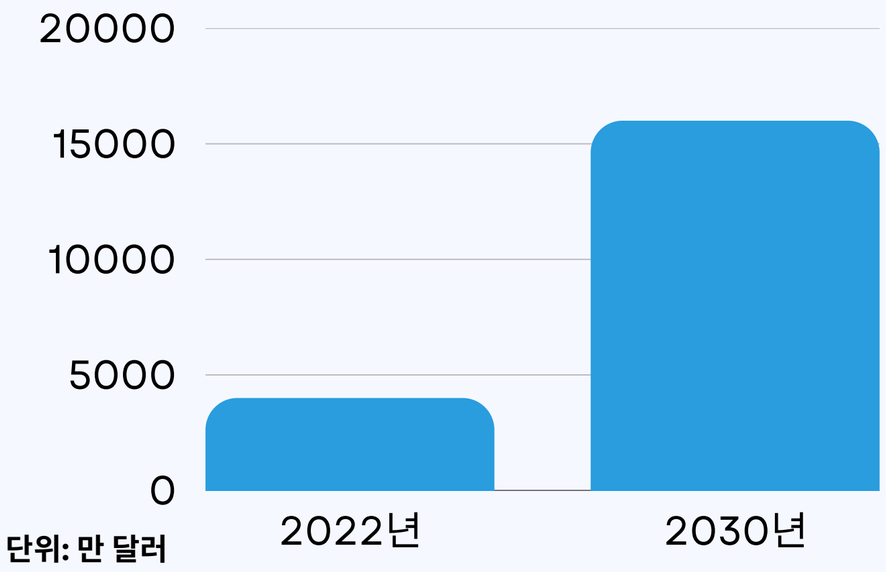


정부는 2025년 UAM 상용화 서비스 개시를 주 내용으로 "한국형 도심항공교통(K-UAM) 기술 로드맵"을 발표

2025년 UAM 상용서비스를 목표로 설정하고 2024년까지 비행실증,
2030년부터 본격 상용화를 준비하는 단계적 목표 제시

UAM 국내 동향

국내 UAM 시장 동향



2022년 약 4000만 달러에서 2030년 약 1억 6000만 달러로 성장할 전망

출처: HTTPS://BRUNCH.CO.KR/@MENTATS1/513

주요 기업

supernal

현대자동차의 슈퍼널은 2028년 연간 200대 생산을 목표로 eVTOL 개발을 진행중

한화시스템

UBER의 PAV 제조협력사인 OVERAIR사의 EVTOL 공동 개발에 25백만달러를 투자 → 2025년 에어택시 시장에 본격적으로 진출 계획

기사: HTTP://WWW.DIGITALBIZON.COM/NEWS/ARTICLEVIEW.HTML?IDXNO=2339306

02

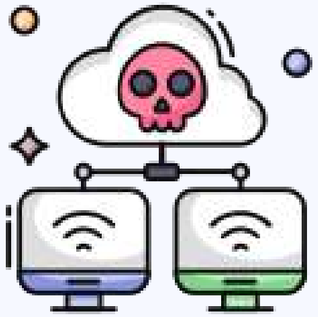
UAM 사이버 위협 분석 (문제점)

"UAM 상용화에 따라 안전한 운항을 저해하는 요소들이 생길 것"

UAM환경에서의 주요 사이버 보안 위협 요소

GPS 위협

네트워크 공격



악성 소프트웨어

데이터 유출

UAM 사이버 위협공격 시나리오

GPS 스푸핑, 재밍

➔ UAM은 GPS를 통해 경로를 설정

➔ GPS신호가 변조되거나 방해를 받음

➔ 기체의 오작동

ex)비행 경로 이탈, 타 기체와 충돌

버티포트 해킹

➔ 버티포트 UTM 시스템 해킹

➔ 공역 통제 불가(항로 조작 등)

➔ 충돌 사고 발생 가능성

악성코드 감염

➔ 인프라 시스템 악성코드 감염

➔ GCS, UTM 시스템 등 접근 및 해킹

➔ 조종 명령 왜곡, 실시간 모니터링 마비

➔ UAM 운항 불가

개인정보 유출

➔ 모바일 앱(예약/탑승) 해킹

➔ 개인 정보 탈취(연락처, 카드 번호 등)

➔ 테러, 피싱, 금융사기 등 피해 발생

※UTM: 무인 항공기 교통 관리 시스템, GCS: 지상 관제 시스템

03

대응방안
(문제해결방안)

사이버 보안

- 사이버 환경에서 다양한 보안 위협으로부터 **조직과 사용자 자산의 운영 영속성을 보장**
- 사이버 보안은 **내, 외부 디지털 위협으로부터 조직을 방어**하고, 사이버 범죄에 대비하여 **데이터 뿐만 아니라 비지니스와 평판을 보호하는 역할**

효과적인 보안 조치는 자산, 고객 및 브랜드를
보호하고 조직의 탄력성과 신뢰성 강화

사이버 보안의 일반적인 목표

기밀성 (CONFIDENTIALITY)	무결성 (INTEGRITY)	가용성 (AVAILABILITY)

UAM 사이버 위협 대응방안

1. UAM 사이버 보안 전문 인력 양성

UAM 사이버 보안 전문 인력 양성 프로그램(12주)

목표: **UAM 시스템 보안 위협 분석, 보안 설계 및 대응능력 확보**

기초 교육 2주	기술 실무 6주	실전 실습 4주
UAM 보안 기초 습득	**핵심 보안 기술 학습**	**시나리오 기반 실습**
UAM 개론, 시스템 구성 이해 항공통신/전자 기초 사이버보안 기본 (암호, 인증, 네트워크 보안) 보안 관련 국제 기준(ICAO, 국토부)	EVTOL 통신 보안, GPS 스푸핑 실습 5G 기반 무선 통신 위협 분석 인증/무결성 기술, OTA 보안 펌웨어 보안 및 코드 서명 실습 항공관제 시스템(CNS) 보안 설계 실습 사이버 공격 시나리오 기반 대응 훈련	**최종 실습 프로젝트(예)** UAM 보안 아키텍쳐 설계 모의 해킹 실전 실습 UTM 통신 프로토콜 취약점 분석

주차별 세부 커리큘럼

UAM 사이버 위협 대응방안

2. 디지털 트윈 기능 기반 대응방안

디지털 트윈: 물리적 객체의 가상 모델

- 객체의 센서에서 전송된 실시간 데이터를 사용하여 동작을 시뮬레이션하고 작업을 모니터링

UAM 기체와 똑같은 복제판 기체를 가상세계 안에 만들어 두는 것을 말하며, 현실에 있는 UAM이 비행을 시작하였을 때 가상세계의 복제판 기체도 동시에 비행하기 시작하여 데이터와 상태를 동일한 상황에서 운행

실시간 연결	공격 시뮬레이션 기능	사전 대응 훈련	AI 학습
UAM 비행 시 디지털 트윈도 실시간으로 동일한 동선으로 가상 비행	해커의 사이버 공격들을 사전에 혹은 동시에 가상 복제판에 시험	UAM의 작동을 멈추지 않고도 여러 시나라오를 시험, 이상 징후 패턴을 미리 학습	공격 시뮬레이션 결과를 AI를 통해 학습, AI가 지속적으로 학습하여 사고 경고 및 자가 대응 가능

UAM 기체를 멈추지 않아도 되며, 해킹을 당하기 전 대비가 가능, 기체마다 최적화된 보안 시스템을 만들 수 있으며, 항시 보안 시뮬레이터 작동과 동일한 효과

UAM 사이버 위협 대응방안

3. 검증쿼리 시스템(스푸핑 대항)

GPS 스푸핑: 해커가 가짜 GPS 신호를 보내, 기체를 가짜 위치로 인식하게 만드는 공격

개념

- **UAM 기체와 관제 센터가 GPS 좌표를 주기적으로 상호 검증**
- **관제 센터는 독립 센서/DB를 통해 해당 좌표의 신뢰성 판단**
- **이상 감지 시 즉시 경고 및 비상 비행모드 전환**

UAM위치 위조 공격 대응을 위한 기체-관제 간의 실시간 검증 기술

➔ 일반적인 GPS수신은 단방향이라 스푸핑 탐지 어려움
➔ 이 시스템은 양방향 통신 기반 검증을 활용해서 스푸핑 여부 감지

UAM 사이버 위협 대응방안

4. UAM사이버 보안 인증 등급제

-기체, 관제 시스템, 통신 장비, 운영사 등을 대상으로 **보안 수준에 따른 인증 등급** 부여
-LEVEL 1-5 등급 ->등급에 따라 비행 고도, 운항제한, 인프라 연동 수준 차등 적용

- 비행고도 제한: 보안 수준이 낮을수록 낙하나 해킹 피해를 줄이기 위해 저고도에서만 운항 허용
- 운항 가능 범위: LEVEL이 높아질수록 도심지나 공항 연계 같은 고위험 지역 운행 가능
- 인프라 연동 수준
  -LEVEL 1-2:최소한의 통신 연동(예: 수동 관제)
  -LEVEL 3-4: 클라우드 연동, 데이터 기반 운영
  -LEVEL 5: V2X, 자율 운항, OTA 포함

보안 수준이 낮은 기업/기체는 자연스럽게 **고위험 지역에서 배제**,
기업이 **상위 등급을 얻기 위해 보안에 투자**를 할 수 밖에 없음

보안등급	비행고도 제한	운항가능범위	인프라연동수준	비고
Level 1(최저)	최대 100M이하	허가된 테스트 구역 내 (지방 외곽 등)	기본 통신 (1:1 관제)만 허용	시험용, 초기 단계 플랫폼
Level 2	최대 150M	소규모 도시 지역 내 일부 허용	기본 통신+위치 추적 연동	낮은 보안 리스크 허용
Level 3	최대 200M	중소도시 전역 운항 가능	클라우드 기반 관제 연동 가능	준실용 단계
Level 4	최대 300M	대도시 주요 구간 포함	스마트 인프라 연동 허용	상용 직전 수준
Level 5(최대)	최대 450M	전국 모든 지역(공항, 도심 포함)	고도 인공지능 연동, 자율 비행 및 OTA 가능	고신뢰 운영체제 필요

04

기대효과 및 결론

기대효과

사전 예방

제시한 대응방안 전부 공통적으로 사고가 나기 전 위협을 식별하고 차단

신뢰 확보

위협을 차단함으로써 UAM을 이용할 국민들의 신뢰성 확보

안전성

통합적 대응으로 UAM 시스템 전반의 안전한 운용 환경 확보

결론

**UAM의 안전한 상용화를 위해 사이버 보안은 필수적이며,
여러 대응방안을 고안하고 사이버 위협으로부터 대응함으로써
미래 항공안전의 핵심 가치를 실현해야함.**

감사합니다.

출처 및 참고문헌

HTTPS://WWW.MARKANY.COM/SECURITYNEWS/?Q=YTOXONTZOJEYOIJRZXL3B3JKX3R5CGUIO3M6MZOIYWXSIJT9&BMODE=VIEW&IDX=18926053&T=BOARD
HTTPS://NAMU.WIKI/W/%EB%8F%84%EC%8B%AC%ED%95%AD%EA%B3%B5%EA%B5%90%ED%86%B5
HTTPS://BRUNCH.CO.KR/@MENTATS1/513#COMMENTS HTTPS://WWW.AUTODAILY.CO.KR/NEWS/ARTICLEVIEW.HTML?IDXNO=419748 HTTP://WWW.DIGITALBIZON.COM/NEWS/ARTICLEVIEW.HTML?IDXNO=2339306
HTTPS://HEESIGHT.COM/ENTRY/UAM-%EC%82%B0%EC%97%85-%EB%8F%99%ED%96%A5-%EB%B0%8F-%EA%B8%80%EB%A1%9C%EB%B2%8C-%ED%91%9C%EC%A4%80%ED%99%94-%EB%B0%A9%ED%96%A5
HTTPS://BLOG.NAVER.COM/BSS2062/223374248419 HTTPS://WWW.DBPIA.CO.KR/JOURNAL/ARTICLEDETAIL?NODEID=NODE11038603 HTTPS://SCIENCEON.KISTI.RE.KR/COMMONS/UTIL/ORIGINALVIEW.DO?CN=JAKO202427039972633&DBT=JAKO&KOI=KISTI1.1003%2FJNL.JAKO202427039972633