# STPA-Sec을 활용한 UAV의 보안 및 안전 요구사항 분석

KSC 2020

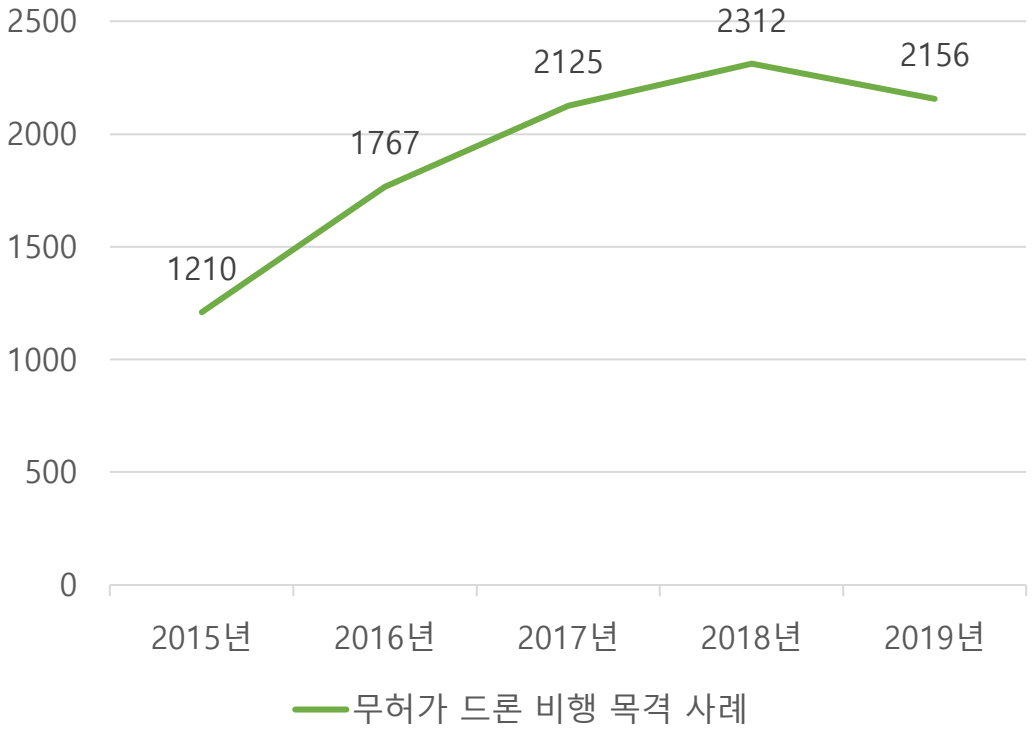
허윤아° 이동아 유준범
건국대학교 컴퓨터공학과

# 목차

1. UAV에서 안전·보안의 중요성
2. STPA-Sec
3. UAV에의 STPA-Sec의 적용
4. 안전 및 보안 요구사항
5. 기존 연구와의 차이점
6. 향후 연구 및 결론

# 1. UAV 안전·보안의 중요성

사고로 이어질 수 있는 드론 비행 사례의 증가




**UAS(UAV System)**[2]

Unmanned Aerial Vehicle[1]

조종사가 비행체에 직접 탑승하지 않고 원격 조종이 가능함

다양한 임무 수행을 위한 장비들을 추가적으로 탑재할 수 있고, 대기권 내에서 임무를 수행할 수 있는 비행체

GCS(Ground Control Station)

Data link

그 외 지원 장비

⇩

사고 발생 시 큰 손실을 미칠 수 있는
safety-critical system

+

무선 통신을 이용하므로 보안에 취약할 수 있음

[1] 이경태, 이기학, 2000 [2] 안진영, 2015 [3] FAA, "UAS Sightings Report"

# 2. STPA-Sec

**STPA**[4] + **Sec**urity

**S**ystem **T**heoretic **P**rocess **A**nalysis
시스템 이론 기반의 위험 분석 기법

안전과 보안 둘 다 시스템 전체 관점에서 보아야 함

STPA-Sec[5] **extends** STPA

*System Engineering Foundations*

- Define and frame security problem
  - Identify losses/accidents
  - Identify system hazards/constraints

*Identify Types of Unsafe/Unsecure Control*

- Model functional control structure
- Identify unsafe/unsecure control actions

*Identify Causes of Unsafe/Unsecure Control and Eliminate or Control Them*

- Trace hazardous control actions using information life cycle
- Identify scenarios leading to unsafe control actions
- Identify scenarios leading to unsecure control actions
- Place scenarios on D4 Chart to ID more critical security scenarios
- Wargame security scenarios to select control strategy
- Develop new requirements, controls, and design features to eliminate or mitigate unsafe/unsecure scenarios

RED = STPA-Sec Extension on STPA

STPA-Sec 수행 과정[6]

[4] Nancy G. Leveson, 2009 [5] William Young, Nancy G. Leveson, 2014 [6] William Young Jr, PhD. Reed Porada, 2017

# 3. UAV에의 STPA-Sec의 적용

**적용 대상** : 이·착륙, 촬영 등 기본적인 기능을 탑재한 소방용 드론

STPA-Sec 수행 → (manually) Scenario를 기반으로 안전 및 보안 요구사항 도출

STPA + STRIDE[7][8]

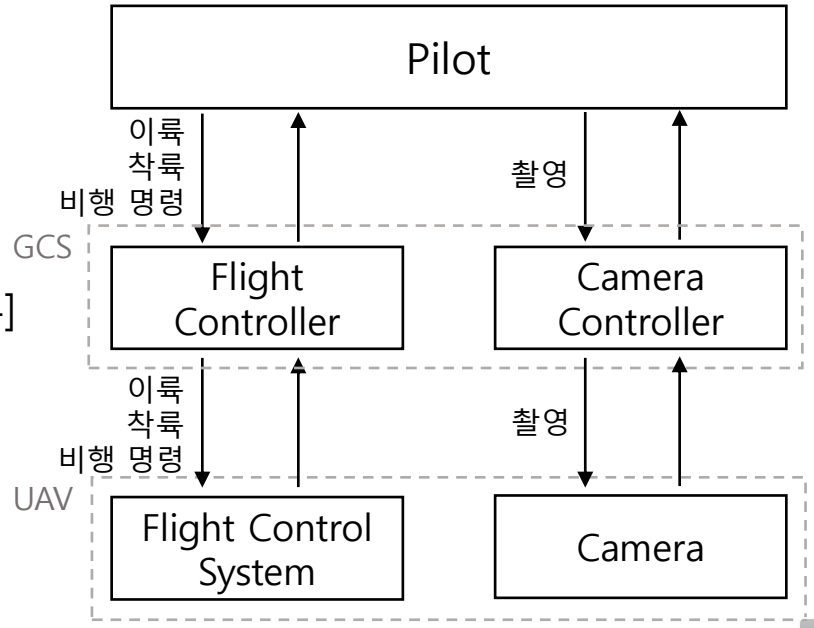
**S**poofing
**T**ampering
**R**epudiation
**I**nformation Disclosure
**D**enial of Service(DoS)
**E**levation of Privilege

## 적용 결과

▷ Loss
1) 인명 피해(사망 또는 부상)
2) 기체 외부 대상의 손실 또는 손상
3) 기체 손실 또는 손상
4) 임무 실패

▷ Hazard
1) 비행 중 지상의 사람 또는 물체와 최소 허용 거리 위반함[L1, L2, L3, L4]
2) 비행 중 다른 비행체와 최소 허용 거리 위반함[L2, L3, L4]
3) 비행 중 드론 제어권을 상실함[L3, L4]
4) 드론이 비행이 허용되지 않은 구역에서 비행함[L1, L2, L3]
5) 드론이 임무 수행 지역에 도달할 수 없음[L4]
6) 임무를 명령한 대로 수행하지 못함[L4]

**control structure 예시**

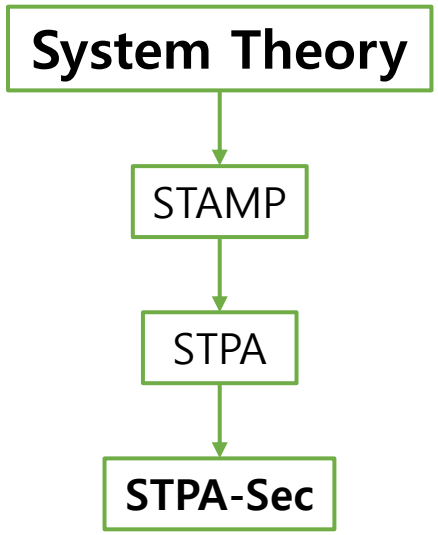



[7] Loren Kohnfelder, Praerit Garg, 2018 [8] Nivio Paula de Souza, et al, 2020

# 4. 안전 및 보안 요구사항

| UCA | Scenario | 안전 요구사항 | STRIDE | 보안 요구사항 |
|---|---|---|---|---|
| **Pilot이 빨리 주어진 임무를 수행해야 하는 상황에서 기체 이륙 명령을 제공하지 않음[H6]** | Pilot은 CA를 제공했으나, flight controller가 통신 문제로 CA를 전달하지 못해서 기체 이륙 명령을 수행하지 않았다. | Flight controller와 Flight control system의 통신 연결은 항상 유지되어야 하고, 주고받는 정보가 정확해야 한다. | T, D | Pilot과 flight controller, flight controller와 flight control system 사이에서 처음 정보를 주고받기 전, 상호 인증을 거쳐야 한다.<br>주고받는 CA가 안전한지, 올바른지 검증할 수 있어야 한다.<br>Flight controller는 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다. |
| | Flight control system이 CA를 수신했으나, 기체 이륙 명령을 수행하지 않았다. | Flight control system은 flight controller로부터 제공받은 이륙 명령을 항상 수행해야 한다. | D | Flight control system은 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다. |
| **Pilot이 배터리 잔량이 부족한 상황에서 기체 착륙 명령을 너무 늦게 제공함[H3]** | Display가 기체의 배터리 잔량 부족을 너무 늦게 출력해서 pilot이 기체 착륙 명령을 너무 늦게 제공했다. | Display는 기체의 배터리 잔량 정보를 일정 시간마다 업데이트하여 출력해야 한다. | S, T, D | 기체의 배터리 잔량 정보를 주고받는 통신에 있어서 기밀성을 갖춰야 한다.<br>Display와 flight control system 사이에서 처음 정보를 주고받기 전, 상호 인증을 거쳐야 한다.<br>Display는 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다. |
| | Flight control system이 CA를 수신하지 못했으나, 수신한 척 기체 착륙 명령을 뒤늦게 수행했다. | Flight control system은 항상 수신한 착륙 명령만 수행해야 한다. | S, T, D | 착륙 명령을 주고받는 통신에 있어서 기밀성을 갖춰야 함<br>Flight control system은 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다. |

# 5. 기존 연구와의 차이점




1. 시스템 단위에서의 분석
2. 인적 요소의 고려

개괄적인 제안[9][10]

인증된 접근만 허가해야 한다
정보의 기밀성을 유지해야 한다
암호 키를 사용해야 한다
…

또는

Component와 interface별로 분류[11]

각 component 별 분석 가능
시스템 전체에 대한 분석 가능

# 6. 향후 연구 및 결론

- **결론**
  - STPA-Sec을 이용한 안전 및 보안 요구사항 도출
  - 안전·보안이 중요한 다른 분야에의 적용 가능성

- **향후 연구**
  - 도출된 안전 및 보안 요구사항을 실제로 적용했을 때 기대되는 효과에 대한 연구

# 참고 문헌


[1] 이경태, 이기학. "UAV 총론 및 국내 UAV 연구개발 방향". 한국항공우주학회지, 28(6), 142-163. 2000.

[2] 안진영. "세계의 민간 무인항공기시스템(UAS) 관련 규제 현황". 항공우주산업기술동향, 13(1), 51-67. 2015.

[3] Federal Aviation Administration(FAA). "UAS Sightings Report".

[4] Nancy G. Leveson. "Engineering a Safer World". MIT Press. 2009.

[5] Young, W., & Leveson, N. G. "An integrated approach to safety and Security based on systems theory". Communications of the ACM, 57(2), 31-35. 2014.

[6] William Young Jr, PhD. Reed Porada. "System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA". 2017 STAMP Conference, Boston, MA. March 27, 2017.

[7] Kohnfelder, Loren; Garg, Praerit. "The threats to our products". Microsoft Interface. April 1, 1999. Retrieved 18 August 2018.

[8] Nivio Paula de Souza, Cecília de Azevedo Castro César, Juliana de Melo Bezerra, Celso Massaki Hirata. "Extending STPA with STRIDE to identify cybersecurity loss scenarios". Journal of Information Security and Applications. Volume 55. 2020,

[9] Riham Altawy and Amr M. Youssef. "Security, privacy, and safety aspects of civilian drones: A survey". ACM Trans. Cyber-Phys. Syst. 1, 2, Article 7 (November 2016), 25 pages. 2016.

[10] Kim, Daegeon, and Huy Kang Kim. "Security Requirements of Commercial Drones for Public Authorities by Vulnerability Analysis of Applications". arXiv preprint arXiv:1909.02786. 2019.

[11] 정보통신단체표준(TTA), "드론 기반 서비스를 위한 보안 요구사항", TTAK.KO-12.0317, 2016.12.