STPA-Sec을 활용한 UAV의 보안 및 안전 요구사항 분석

허윤아[O] 이동아 유준범
건국대학교 컴퓨터공학과
hyoona1202@naver.com, ldalove@konkuk.ac.kr, jbyoo@konkuk.ac.kr

An approach to analyze Security and safety requirement for UAV using STPA-Sec

Yoon-A Heo[O] Dong-Ah Lee Junbeom Yoo
Konkuk University, Division of Computer Science and Engineering

요 약

최근 UAV의 사용이 급격하게 증가하면서, 사고의 빈도 또한 대폭 증가했다. UAV는 사고가 발생할 경우 막대한 피해를 초래할 수 있으므로, 보안 및 안전 요구사항을 분석할 필요가 있다. 본 논문에서는 STPA-Sec을 활용해 UAV의 안전 및 보안에 대해 분석을 수행하고 안전 및 보안 요구사항을 도출한 결과를 제시하였다. 또한 기존의 연구와 본 논문에서 사용한 요구사항 도출 방법을 비교·분석했다.

1. 서 론

UAV(Unmanned Aerial Vehicle)란, 조종사가 비행체에 직접 탑승하지 않고 원격 조종이 가능하며(unmanned), 다양한 임무 수행을 위한 장비들을 추가적으로 탑재할 수 있고, 대기권 내에서 임무를 수행할 수 있는 비행체(aerial vehicle)를 의미한다.[1] UAV 시스템은, 앞서 서술한 UAV와 임무를 위한 장비, 지상통제장비(GCS: Ground Control Station) 및 데이터 링크, 지원 장비 등을 포함한 전체 시스템을 통칭한다.[2] 최근 UAV의 사용이 증가하면서, 사고의 빈도 또한 증가했다.[6] 그런데 UAV 시스템은, 시스템에 문제가 발생할 경우 인명 피해나 재산 손실 등의 큰 손실을 미칠 수 있는 safety-significant system이다. 또한, UAV는 무선 통신을 통해 신호를 받아 동작하므로 보안 측면에서도 분석할 필요가 있다.

UAV 시스템은 안전과 보안이 모두 중요한 시스템이므로, 안전성과 보안성을 통합해 분석할 필요가 있다. 또한, 기능안전성 표준에서도 보안 및 안전에 대한 분석을 요구하고 있다. 안전이나 보안 측면을 살펴보기 위해서는, 시스템을 component 단위로 분류하지 않고 시스템 전체로 살펴보는 것이 필요하다. 본 논문에서는 안전성과 보안성을 통합해서 분석하기 위해서, STPA-Sec을 활용해서 UAV의 안전 및 보안에 대해 분석을 수행하고, 안전 및 보안 요구사항의 분석을 진행할 것이다. 그리고 기존에도 UAV의 안전성 확보를 위해 다양한 연구들이 진행되어 왔으므로, STPA-Sec를 통해 분석한 내용은 기존의 분석 결과와 어떤 차이점을 가지고 있는지 살펴보고, 안전 및 보안 요구사항의 도출 방법에 대한 고찰할 것이다.

2. STPA-Sec

STPA-Sec[4]은 안전 관점에서만 분석 가능한 STPA의 한계를 해소할 수 있도록 보안 관점에서도 분석 가능하게 확장한 것이다. STPA에 그 기반을 두고 있으므로 대부분의 과정은 STPA와 유사하다. 그림 1을 통해 STPA-Sec의 수행 과정과, STPA-Sec과 STPA와의 차이점을 알 수 있다.

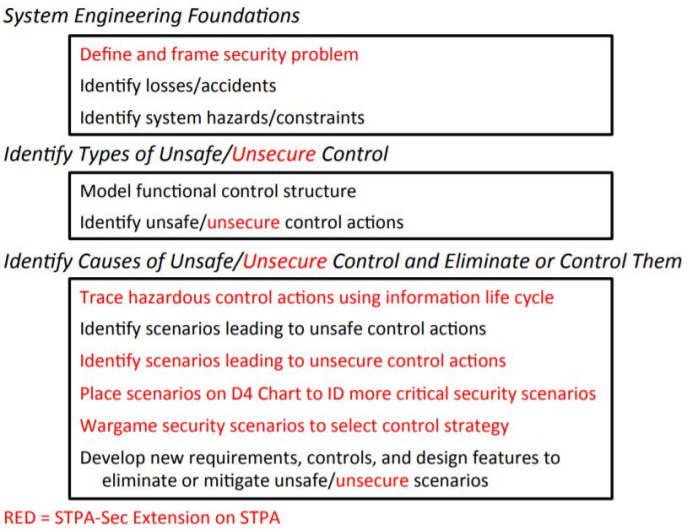

그림 1 STPA-Sec 수행 과정[1]

STPA-Sec을 통해서 가장 먼저 loss/accident와 system-level hazard를 도출해낼 수 있다. 여기서 loss/accident는 실제 발생할 수 있는 사고를 의미하고, hazard는 각 loss/accident의 원인에 해당한다. 하나의

[1] (William Young Jr, PhD. Reed Porada 2017, 25)

hazard가 다양한 loss/accident의 원인이 될 수 있다. 분석한 hazard는 system-level의 constraint로 전환한다.

다음으로 control structure을 작성한다. 세 번째 단계에서는 이 control structure에서 얻어지는 control action과 분석한 hazard를 활용해 Unsafe/Unsecure control action(UCA)을 도출하는 과정을 거친다. UCA를 분석할 때 첫 번째 행은 control structure 도식화를 통해 얻은 control action(CA)에 해당하고, 두 번째 행부터 다섯 번째 행은 각각의 UCA type에 해당하는 결과물에 해당한다. 이후 각 UCA에 대한 unsafe/unsecure scenario를 4가지 종류의 causal factor를 통해 도출해낼 수 있다.

이후 wargaming을 통해 유의미한 제약사항들을 도출할 수 있도록 한다. unsafe/unsecure scenario를 완화시키기 위해 수행한 과정들을 다시 반복하는 것이 전체적인 STPA-Sec의 과정이다.

3. STPA-Sec을 적용한 안전 및 보안 요구사항 도출

본 논문에서 분석의 예시로 활용하는 UAV는 이륙, 착륙, 촬영 등의 기본적인 기능을 가지고 있는 소방용 드론이다. 해당 UAV에 대한 STPA-Sec을 수행한 이후에는, 도출된 scenario를 기반으로 manual하게 안전 및 보안 요구사항을 도출한다. Scenario를 통해 hazard를 효과적으로 완화할 수 있는 요구사항을 역으로 도출하는 것이다.

단, 본 논문에서는 앞서 설명한 STPA-Sec의 절차 중 일부 과정에 다른 방법을 사용하였다. STPA를 보안 측면으로 확장하는 또 다른 방법으로 STPA 과정[3]을 수행한 이후에 STRIDE 모델[5]을 통해 시스템에 가해질 수 있는 threat을 분석하도록 했다.[10] 이 방법을 따라 먼저 STPA를 적용해서 loss와 hazard를 분석한 결과는 아래와 같다.

▷ Loss
- L1) 인명 피해(사망 또는 부상)
- L2) 기체 외부 대상의 손실 또는 손상
- L3) 기체 손실 또는 손상
- L4) 임무 실패

▷ Hazard
- H1) 비행 중 지상의 사람 또는 물체와 최소 허용 거리 위반함[L1, L2, L3, L4]
- H2) 비행 중 다른 비행체와 최소 허용 거리 위반함[L2, L3, L4]
- H3) 비행 중 드론 제어권을 상실함[L3, L4]
- H4) 드론이 비행이 허용되지 않은 구역에서 비행함[L1, L2, L3]
- H5) 드론이 임무 수행 지역에 도달할 수 없음[L4]
- H6) 임무를 명령한 대로 수행하지 못함[L4]

이후 control structure를 작성하고, UCA를 도출했다. 각 UCA에 대해 unsafe/unsecure scenario를 작성하고

표 1 STPA-Sec 을 통한 안전 및 보안 요구사항 도출

UCA	Scenario	안전 요구사항	STRIDE	보안 요구사항
Pilot 이 빨리 주어진 임무를 수행해야 하는 상황에서 기체 이륙 명령을 제공하지 않음[H6]	Pilot 은 CA 를 제공했으나, flight controller 가 통신 문제로 CA 를 전달하지 못해서 기체 이륙 명령을 수행하지 않았다..	Flight controller 와 Flight control system 의 통신 연결은 항상 유지되어야 하고, 주고받는 정보가 정확해야 한다.	T, D	Pilot 과 flight controller, flight controller 와 flight control system 사이에서 처음 정보를 주고받기 전, 상호 인증을 거쳐야 한다. 주고받는 CA 가 안전한지, 올바른지 검증할 수 있어야 한다. Flight controller 는 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다.
	Flight control system 이 CA 를 수신했으나, 기체 이륙 명령을 수행하지 않았다.	Flight control system 은 flight controller 로부터 제공받은 이륙 명령을 항상 수행해야 한다.	D	Flight control system 은 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다.
Pilot 이 배터리 잔량이 부족한 상황에서 기체 착륙 명령을 너무 늦게 제공함[H3]	Display 가 기체의 배터리 잔량 부족을 너무 늦게 출력해서 pilot 이 기체 착륙 명령을 너무 늦게 제공했다.	Display 는 기체의 배터리 잔량 정보를 일정 시간마다 업데이트하여 출력해야 한다.	S, T, D	기체의 배터리 잔량 정보를 주고받는 통신에 있어서 기밀성을 갖춰야 한다. Display 와 flight control system 사이에서 처음 정보를 주고받기 전, 상호 인증을 거쳐야 한다. Display 는 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다.
	Flight control system 이 CA 를 수신하지 못했으나, 수신한 척 기체 착륙 명령을 뒤늦게 수행했다.	Flight control system 은 항상 수신한 착륙 명령만 수행해야 한다.	S, T, D	착륙 명령을 주고받는 통신에 있어서 기밀성을 갖춰야 함 Flight control system 은 서비스 거부(DoS) 공격에 대한 저항성을 갖춰야 한다.

나서는 각 scenario에 대한 안전 요구사항을 먼저 작성했다. 그리고 scenario에 대해 STRIDE 모델을 적용한 후 보안 요구사항을 작성했다. 표 1은 분석을 진행한 예시 중 일부이다.

4. STPA-Sec을 적용한 안전 및 보안 요구사항에 대한 고찰

STPA-Sec은 다른 기법들과는 달리 시스템 이론에 기반을 두고 있으므로 시스템 단위에서 분석 가능하다는 특징이 있다. 이런 점 때문에 각 component 단위에서 시스템을 분석할 때는 볼 수 없었던 점들을 살펴볼 수 있다. 또, 인적 요소 또한 고려하기 때문에 UAV를 조종하는 pilot에 대한 요구사항도 분석할 수 있다. 단, STRIDE 모델을 활용해서 보안 요구사항을 작성할 때는 인적 요소에 대한 것을 고려하는 것이 어렵다.

기존에 제안되었던 보안 요구사항을 살펴보면, '인증된 접근만 허가해야 한다', '정보의 기밀성을 유지해야 한다', '암호 키를 사용해야 한다' 와 같이 큰 틀에서 제안하거나[7][8], 각 component와 interface 별로 분류해서 제안하는[9] 형식이었다. 앞서 STPA-Sec을 적용해 제안한 보안 요구사항은 각 component 별로 살펴볼 수 있는 동시에, 시스템 전체에 대한 분석 또한 빠짐없이 살펴볼 수 있다는 점에서 기존의 보안 요구사항과 차이점이 있다.

5. 향후 연구 및 결론

본 논문에서는 STPA-Sec를 이용하여 안전 및 보안 요구사항을 분석하고 도출해, 기존에 제시되었던 요구사항들과 비교했다. 요구사항을 도출하는 데에 활용한 방법은 UAV 뿐만 아니라 다른 분야에서도 사용할 수 있을 것이다. 향후 연구로는 이렇게 도출한 안전 및 보안 요구사항을 실제로 UAV 시스템에 도입했을 때 기대되는 효과에 대해 연구할 계획이다.

사 사

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업(NRF-2017M3C4A7066479)과 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업 (No.2018-0-00213, SW중심대학(건국대학교))의 지원을 받아 수행된 연구임

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

[4] 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.

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

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

[7] 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.

[8] 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.

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

[10] 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,

[11] 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.