위험원 분석기법을 활용한 공공임무용 무인이동체시스템에 대한 안전 요구사항의 도출에 관한 연구

임상연*, 김상헌*, 정호전*, 박진규*, 방승재*
*한국산업기술시험원
e-mail:isy0619@ktl.re.kr

A study on the deriving safety requirement for unmanned aircraft vehicle using hazard analysis technique

Sang-Yeon Lim* , Sang-Hun Kim*, Jin-Kyu Park*, Seung Jae Bang*
*Dept. of System Verification and Validation Center, Korea Testing Laboratory

요 약

다양한 분야에서 무인이동체시스템이 활용됨에 따라 안전성에 대한 우려가 높아지고 있다. 최근 무인이동체시스템은 공공 및 민간분야에서 다양한 활용을 위한 연구가 진행되고 있다. 특히 재난·치안, 소방 진압, 우편물 배송 등 공공분야 활용을 위한 적용 연구가 수행되고 있으며, 상업적으로는 레저, 영상촬영을 위한 무인이동체 개발이 진행되고 있다. 그러나 다양한 활용을 위한 연구 및 개발, 나아가 실용화 진행됨에도 불구하고 무인이동체의 안전에 대한 위험위험 분석 및 그에 따른 안전요구사항 반영이 미비한 실정이다. 이를 위해 무인이동체시스템을 대상으로 특정 운용환경에서 위험원 분석 및 그에 따른 안전대책을 분석하여 안전요구사항을 도출, 이를 설계 및 제작에 반영한 안전확보에 대한 연구가 필요하다.

본 논문에서는 공공분야에서 활용을 목적으로 개발되는 무인이동체시스템에 대해 대표적 위험분석 기법인 HAZOP을 활용한다. HAZOP기법 적용을 통해 특정 운용환경을 반영한 정상상태 시나리오를 도출하여 위험원을 도출하고, 이에 대한 안전확보 대책을 수립하여 최종적으로 안전요구사항을 도출한다. 이를 위해 무인이동체시스템의 정상상태 시나리오 도출 및 특정운용환경 분석 및 적용, 각 시나리오별 위험원 분석 및 그에 따른 안전대책 및 최종적으로 안전 요구사항을 도출하였다. 도출된 안전 요구사항은 향후 공공목적 또는 상업용으로 활용되는 무인이동체시스템의 설계 및 제작단계에 반영되어 안전확보가 가능할 것으로 기대한다.

1. 서론

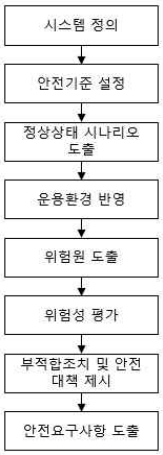
국내·외 무인이동체시스템 분야의 활성화에 따라 다양한 분야에서 무인이동체시스템 적용에 대한 활발한 연구 및 개발이 진행되고 있다. 국제적으로는 첨단기술의 융합산업 및 최대 유망시장으로서 미국, 중국, 유럽 등 나라별로 시장선점을 위한 경쟁이 이루어지고 있으며, 국내에서는 군수를 중심으로 잠재력이 큰 민수시장으로의 진출이 진행되고 있다. 특히 국내에서는 재난·치안 등 공공분야의 무인이동체시스템 적용에 대한 연구가 활발히 진행되고 있으며, 민수시장에서는 대한항공 및 유콘시스템 등이 자체개발을 통해 무인이동체를 개발, 군수시장에서 사업을 추진하고 있다. [1,2]

그러나 이러한 국내·외 적으로 무인이동체 시장에 대한 높은 관심 및 치열한 투자에도 불구하고 무인이동체시스템의 안전에 대한 위험분석 및 안전대책 수립은 미비한 수준이다. 최근 사업용 뿐만아니라, 취미 레저용 무인이동체시스템 추락에 따른 인사 및 상해사고가 증가하고 있으며, 이에 따른 안전확보 필요성에 대한 요구가 높아지고 있다.

본 논문에서는 무인이동체시스템의 안전대책확보를 위한 위험원 식별 등의 위험분석을 수행하였다. 전통적인 위험분석 기법인 HAZOP을 적용하여 특정운용환경을 반영한 정상상태 시나리오를 도출, 특정 운용환경을 분석 및 적용하여 각 시나리오별 위험원 분석 및 그에 따른 안전대책 및 최종적으로 안전요구사항을 도출하였다.

2. 위험 분석 기법 적용

2.1 위험분석기법(HAZOP)을 활용한 위험원 분석 절차



[그림 1]위험분석기법(HAZOP) 기법을 활용한 위험분석 절차

무인이동체시스템의 위험분석을 위해 전통적인 위험분석 기법인 HAZOP을 적용하였다. HAZOP 기법은 시스템에 잠재되어 있는 위험원을 식별하기 위한 구조화되고 체계적인 기법으로 설계 또는 운영 의도로부터 이탈(Deviation)에 의해 위험사건을 가정하여 정상상태에서 이탈을 식별한다.[3]

무인이동체시스템의 위험분석은 무인이동체시스템 정의 후 그에 따른 안전기준 설정으로 시작한다. 이후 무인이동체시스템의 정상상태 시나리오를 도출, 운용환경 특성을 반영하여 위험원 도출 및 평가를 수행한다. 이를 통해 부적합사항을 식별하고 그에 따른 안전대책을 제시한다. 최종적으로 안전대책을 종합하여 안전요구사항을 도출한다.

2.2 무인이동체시스템 대상 Guideword 및 Parameter 정의

무인이동체시스템의 위험분석 전 안내어(Guideword) 및 변수(Parameter)을 정의한다, 이는 무인이동체시스템의 정상상태 시나리오에서 발생되는 이탈상황에 대해 안내어 및 변수 조합을 통해 해당시스템의 이탈을 도출하기 위함이다.

[표 1] 무인이동체 대상 Guideword

유형	안내어	정의
부정	No	명령이 실행되지 않음
정량적 변화	More	수량의 비정상 증가
	Less	수량의 비정상 감소
정성적변화	As well as	기대하지 않은 동작 수행
	Part of	완전한 수행을 하지 못함
대처	Reverse	목적과 반대되는 결과 도출
	Other than	목적과 다른 결과 도출
시간	Early	예상시간 보다 일찍 발생
	Late	예상보다 늦게 발생
명령 또는 흐름	Before	예상순서보다 일찍 발생
	After	예상순서보다 늦게 발생

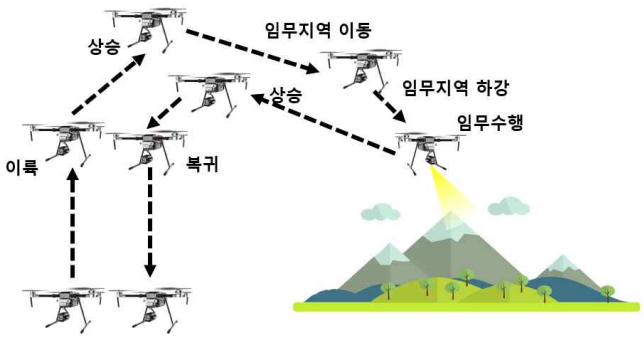
[표 2] 무인이동체 대상 Parameter

Parameter	설명
Interface	무인이동체와 GCS간 통신 인터페이스
Direction	무인이동체 임무비행 방향
Distance	임무거리 및 통신반경
Speed	최대수평비행 속도 및 상승속도
Thrust	모터, 프로펠러 사이즈, 기체 중량 정보 등
Environment	도서산간 지역
Manoeuvre	제어명령, 자동임무수행, 장애물감지 및 회피 수행

2.3 정상상태 시나리오 도출 및 적용

무인이동체시스템의 위험분석을 위한 정상상태 시나리오를 도출한다. 도서산간지역을 운용환경을 갖는 무인이동체시스템으로 가정하여 기본이되는 정상상태 운용시나리오를 도출한다.

정상상태 시나리오는 무인이동체가 이륙 후 상승하여 임무지역으로 이동한 후 하강하여 임무를 수행하는 기본적인 시나리오이다.



[그림 2] 정상상태 임무 운영시나리오 도출

2.3 Hazard log 도출

안내어 및 변수를 조합하여 정상상태 임무운용시나리오에 적용하여 위험분석을 수행한다. 이륙, 상승, 임무지역 이동, 임무지역 하강, 임무수행, 상승, 복귀의 임무 시나리오에 따라 발생될 수 있는 이탈상황을 정의한다. 다음 표3에서 무인이동체시스템에 대한 Hazard log를 정의하였다.

2.4 안전대책 및 안전요구사항 도출

도출된 Hazard log를 통해 부적합사항을 식별하고 이를 경감할 수 있는 안전대책을 도출한다. 각 시나리오에서 발생되는 이탈상황에 대한 안전대책을 식별하고 정제하여 안전요구사항을 최종적으로 도출한다.

Action	Parameter	Guideword	Deviation	Causes	Description	Consequences	Mitigation
이륙	Interface	No	Interface 불가	무인이동체 통신 불가	무인이동체의 조종신호, 위치 정보 등의 송·수신 불가로 제어가 불가능함	무인이동체 이륙 불가	비행 전 기초작동점검 수행
	Thrust	Less	모터 토크 출력 저하	부족한 무인비행체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 이륙 불가	주기적인 모터상태 확인
		As well as	프로펠러 회전 수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 이륙 불가	주기적인 프로펠러 상태 확인
	Manoeuvre	Part of	명령수행 불가	이륙명령을 수행하지 못함	이륙명령을 수신하였으나, 수행하지 못함	무인이동체 이륙 불가	비행 전 기초작동점검 수행
상승	Thrust	Less	모터 토크 출력 저하	부족한 무인이동체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
		As well as	프로펠러 회전수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
임무지역 이동	Distance	More or Less	비정상 거리정보 수신	무인이동체 위치 이동	무인이동체의 잘못된 위치수신으로 인해 위치 이동	무인이동체 충돌 무인이동체 상실	무인이동체 조종안정성, 비행안정성 기능 적용
	Interface Environment	Part of	Interface 불가	무인이동체 통신 불가	무인이동체의 도서환경에서의 통신이 불완전함	무인이동체 상실	통신두절에 대한 대응절차 수행
임무수행 고도 하강	Thrust	Less	모터 토크 출력 저하	부족한 무인이동체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 임무수행 고도 하강 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
		As well as	프로펠러 회전수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 임무수행 고도 하강 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
	Envirionment	Part of	Interface 불가	무인이동체 통신 불가	무인이동체의 도서환경에서의 통신이 불완전함	무인이동체 상실	통신두절에 대한 대응절차 수행
임무수행	Thrust	Less	모터 토크 출력 저하	부족한 무인이동체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 임무수행 고도 하강 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
	As well as	프로펠러 회전수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 임무수행 고도 하강 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용	
	Envirionment	Part of	Interface 불가	무인이동체 통신 불가	무인이동체의 도서환경에서의 통신이 불완전함	무인이동체 상실	통신두절에 대한 대응절차 수행
상승	Thrust	Less	모터 토크 출력 저하	부족한 무인이동체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
		As well as	프로펠러 회전수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
복귀	Distance	More or Less	비정상 거리정보 수신	무인이동체 위치 이동	무인이동체의 잘못된 위치수신으로 인해 위치 이동	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
	Interface Environment	Part of	Interface 불가	무인이동체 통신 불가	무인이동체의 도서환경에서의 통신이 불완전함	무인이동체 상승 후 제자리비행 불가	이상상황 감지 및 이상대응 절차 적용
착륙	Thrust	Less	모터 토크 출력 저하	부족한 무인이동체 양력 및 추력	무인이동체의 모터 토크 부족으로 인한 양력 및 추력 부족	무인이동체 착륙 불가	이상상황 감지 및 이상대응 절차 적용
	As well as	프로펠러 회전수 저하	프로펠러 마모 또는 파손	무인이동체 프로펠러의 마모 또는 파손으로 인한 비정상 운행	무인이동체 상승 후 제자리비행 불가	무인이동체 착륙 불가	이상상황 감지 및 이상대응 절차 적용

[표 3] 안전대책 및 안전요구사항 도출

구분	안전대책	안전요구사항
이륙	기초작동점검수행	비행 전 기초작동점검을 수행하여야 한다.
	주기적 모터점검	주기적인 모터점검을 수행하여야 한다.
	주기적 프롭점검	주기적인 프롭점검을 수행하여야 한다.
상승	기초작동점검수행	비행 전 기초작동점검을 수행하여야 한다.
	이상상황 감지 및 대응	이상상황 대응절차를 설계 및 적용하여야 한다.
임무지역 이동	기초작동점검수행	비행 전 기초작동점검을 수행하여야 한다.
	조종 및 비행안정성 기능	조종 및 비행안정성 기능이 설계 적용되어야 한다
임무수행 수행 고도 하강	기초작동점검수행	비행 전 기초작동점검을 수행하여야 한다.
	이상상황 감지 및 대응	이상상황 대응절차를 설계 및 적용하여야 한다.
임무수행	이상상황 감지 및 대응	이상상황 대응절차를 설계 및 적용하여야 한다.
	통신두절 대응	통신두절대응기능이 설계 및 적용되어야 한다.
상승	이상상황 감지 및 대응	이상상황 대응절차를 설계 및 적용하여야 한다.
복귀	기초작동점검수행	
	이상상황 감지 및 대응	이상상황 대응절차를 설계 및 적용하여야 한다.

3. 결론

운영환경을 반영한 무인이동체시스템의 정상 상태 시나리오를 도출하고, 위험분석 방법인 HAZOP을 적용하여 각 시나리오별 이탈을 식별하였으며, 이를 기반으로 무인이동체시스템의 운영시 발현 가능한 위험원들을 식별하였다. 또한 위험원의 원인 및 결과를 분석하고, 위험원들에 대한 경감대책을 식별하여 이를 설계에 적용하기 위한 안전요구사항을 도출하였다. 이를 통해 향후 무인이동체시스템 설계과정에서 안전요구사항을 반영함으로써 무인이동체시스템의 안전을 확보할 수 있을 것이다.

감사의 글

본 논문은 과학기술정보통신부/산업통상자원부/국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음.(과제번호 21DPIW-C153651-03)

참고문헌

[1] JARUS, 'Specific operations Risk Assessment(SORA)', 2.0, 2019년

[2] IEC 61508 (2015) Functional safety of electrical

/electronic/programmable electronic safety-related systems

[3] Jong-gyu, Hwang., Hyun-jeong, Jo., Chan-hee, Han., Woo-sik, Cho., Jin, An., Dong-myeong, Ha., 2010, “A Study on the HAZOP-KR for Hazard Analysis of Train Control Systems