
Research Proposal


Project Name	Fuzz Testing을 통한 위성 SW 분석
-----------------	---------------------------

05 조

202002473 김승혁

201902733 이정윤

202002699 조민기

지도교수: 이성호 교수님  (서명)

Document Revision History

REV#	DATE	AFFECTED SECTION	AUTHR
1	2025/03/11	초고 작성	김승혁
2	2025/03/13	프로젝트 명 정정	김승혁

Table of Contents

목차

1.	연구 주제 이름	5
2.	연구 배경 및 관련 연구.....	5
3.	프로젝트 수행자의 의도.....	6
4.	탐구 내용 및 기대 결과.....	6
5.	프로젝트 관련 학습 계획	7
6.	연구 일정 계획	7

List of Figure

그림 목차 항목을 찾을 수 없습니다.

1. 연구 주제 이름

Fuzz testing을 통한 위성 SW 분석

2. 연구 배경 및 관련 연구

위성 SW는 높은 신뢰성과 안정성이 요구되는 분야로, 오류 발생 시 심각한 경제적·사회적 손실을 초래할 수 있다. 최근에는 오픈소스 위성 SW의 수요와 공급이 많아짐에 따라, 다양한 기여자들의 참여로 빠르게 개발이 이루어지고 있다. 이러한 불특정 다수가 함께 개발하는 상황에서는 다양한 케이스에 대한 철저한 검증이 필수적이며, 이러한 배경에서 Fuzz Testing은 예측하기 어려운 입력을 자동으로 생성하여 SW의 취약점을 탐지하는 강력한 기법으로 주목받고 있다.

위 내용과 관련하여 발표된 기존 연구 내용은 아래와 같다.

2.1 위성 SW 검증의 중요성

위성 SW는 지구 관측, 통신, 내비게이션 등 다양한 분야에서 필수적인 역할을 한다. 소형 위성은 개발 예산이 제한적인 경우가 많고, 대형 위성은 운용 기간이 긴 경우가 많아, 각각의 안정성을 높이기 위해 효율적이고 확실한 소프트웨어 검증방법이 필요하다. 특히 위성은 오류 발생 시 복구가 어렵기 때문에 Fuzz Testing을 통해 사전에 소프트웨어 버그와 취약점을 탐지하는 것이 필수적이다.

2.2 Fuzz Testing의 유효성

기존 연구에서는 정형 기법, 모델 기반 검증, 테스트 자동화 등의 방법이 활용되었지만, 모든 잠재적 결함을 탐지하는 데는 한계가 존재한다. Fuzz Testing은 기존 테스트 기법과 달리 예기치 않은 입력을 대량 생성하여 SW의 안정성을 검증하는 방식이다. 연구에 따르면, Fuzz Testing은 기존의 코드 리뷰나 정적 분석 기법으로는 발견하기 어려운 다양한 버그를 탐지하는 데 효과적임이 입증되었다.

2.3 Fuzz Testing을 통한 버그 발견 사례

Fuzz Testing이 실제 소프트웨어 보안 검증에서 효과적이라는 점은 여러 연구에서 확인되었다. 한 연구에서는 CubeSat 위성 테스트 과정에서 기존 방식으로는 일부 오류를 발견하지

못하는 한계를 지적하며, 연구진이 자동으로 문제를 찾아내는 Fuzz Testing 기법을 개발해 적용했다. 그 결과, 칠레 대학에서 개발 중인 세 개의 CubeSat에서 기존 방법으로 찾지 못했던 12개의 오류를 단 3일 만에 발견하고 신속히 수정할 수 있었다. 이 방법은 위성뿐만 아니라 유사한 구조를 가진 다른 시스템에도 적용할 수 있다.

3. 프로젝트 수행자의 의도

미래 7대 산업에 포함된 우주 항공 분야에서, Fuzzer를 이용한 위성 검증에 대한 연구의 비중이 적다. 본 연구는 Fuzz Testing을 통해 위성 SW의 취약점을 더욱 효과적으로 식별하고, 이에 대한 해결책을 제시하려는 목표를 가지고 있다.

4. 탐구 내용 및 기대 결과

이 연구는 NASA와 ESA가 제공하는 오픈소스 위성 소프트웨어를 수집하여 분석하고 현존하는 Fuzzer 도구들을 적용해 테스트하는 것을 목적으로 한다. 연구 과정에서 오픈소스 소프트웨어의 이슈를 분석하여 버그 발견 과정을 파악하고, Fuzzer가 이를 효과적으로 찾아낼 수 있었는지 또는 미처 발견하지 못한 버그가 있는지 확인한다. Fuzzer를 통해 버그를 발견한 경우에는 Fuzz Testing의 유효성을 입증하고, 발견하지 못한 경우에는 Fuzzer의 개선점을 파악하여 제시함으로써 궁극적으로 Fuzz Testing 연구 및 위성 소프트웨어 검증에 더 효과적인 Fuzzer 개발에 기여하고자 한다.

5. 프로젝트 관련 학습 계획

학습할 내용	기간	역할 분담
연구 관련 논문 수집 및 분석	1주차	전원 담당
오픈소스 위성 SW 수집 및 분석	2주차	전원 담당
Fuzzing 도구 수집 및 분석	3주차	전원 담당
학습 내용 공유 및 검토	4주차	전원 담당

6. 연구 일정 계획

조사할 내용	기간	역할 분담
사전조사 및 문제점 파악	1주차 ~ 4주차	전원 담당
요구사항 정립	5주차	전원 담당
사용사례 조사 및 적용 연구	6주차 ~ 7주차	전원 담당
연구 결과 작성	9주차	전원 담당
연구 논의 작성	10주차	전원 담당
논문 초안 작성	12주차	전원 담당

Related Work Summary Table

번호	연구 제목(저자)	저널/컨퍼런스 (연도)	주요 내용 요약	주요 인사이트
1	Survey of Verification and Validation Techniques for Small Satellite Software Development	IEEE / Space Tech Expo Conference (2015)	소형 위성 소프트웨어 검증의 중요성과 다양한 검증 방법의 이점에 대한 연구	위성 SW 검증의 중요성
2	Fuzzing: State of the Art	IEEE / - (2018)	Fuzzing의 과정과 분류, 주요 문제점 및 최신 해결 기술 분석. 주로 사용되는 Fuzzing Tool을 조사하여 향후 연구 방향 제시	Fuzz Testing의 유효성
3	Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software for Agile Mission Development	IEEE / - (2021)	Fuzz testing 기법을 CubeSat 비행 소프트웨어에 적용하여 기존 방식으로 발견하지 못한 버그들을 빠르게 식별함으로써 개발 중단 없이 테스트 완전성을 향상시켰다.	Fuzz Testing을 통한 버그 발견 사례