Fuzz Testing을 통한 위성 SW 분석

종합설계1 5조

202002473 김승혁

201902733 이정윤

202002699 조민기

위성 결함 탐지의 중요성

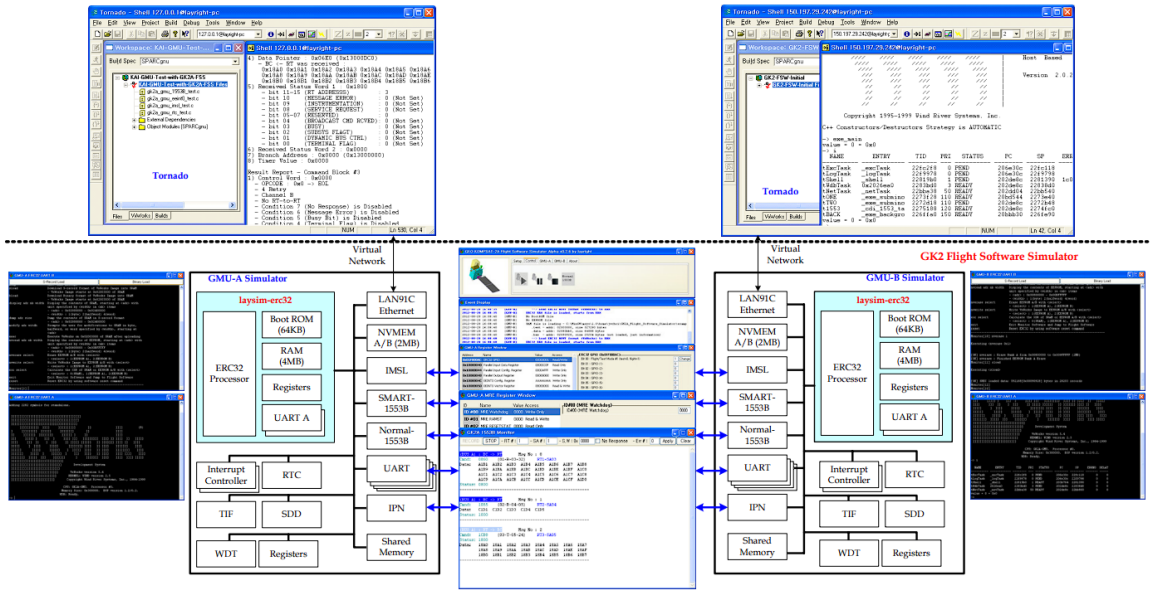
왜 중요한가?

- 우주라는 극한 상황
- 다양한 탑재체 및 시스템 통신
- 오류에 대한 위험 비용 막대함
- 오류 발생 시 복구 힘듬
- 최근 급격하게 늘어난 오픈소스 위성 소프트웨어의 공급과 수요

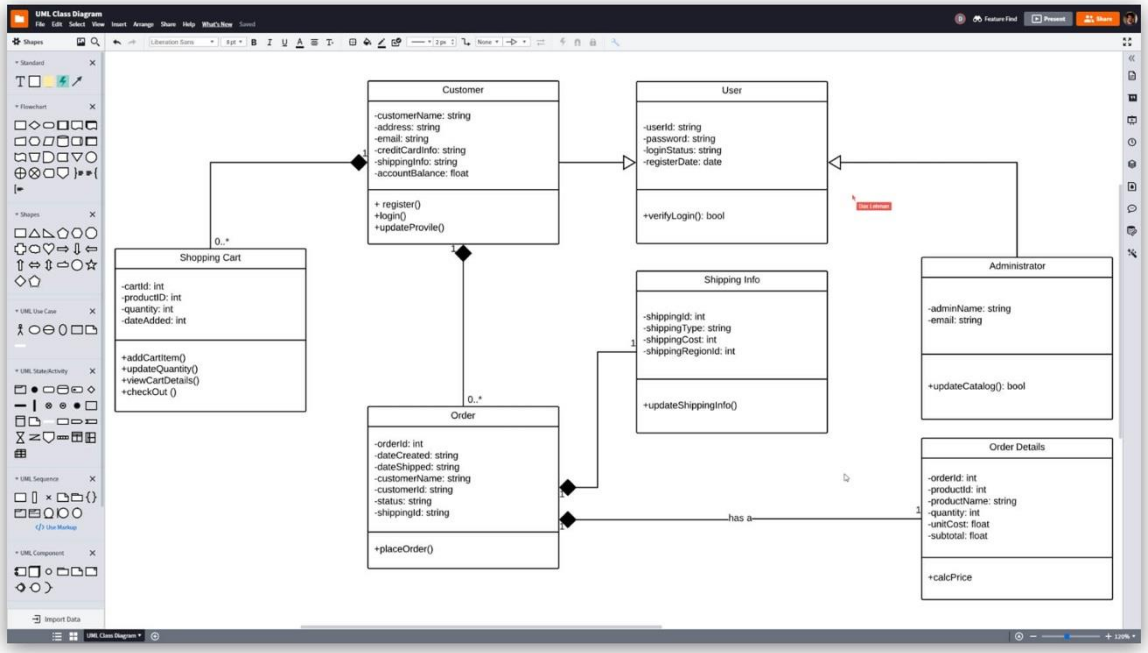
KAI 중형 위성 2호

Fuzz Testing을 통한 결함 탐지

기존 연구의 한계



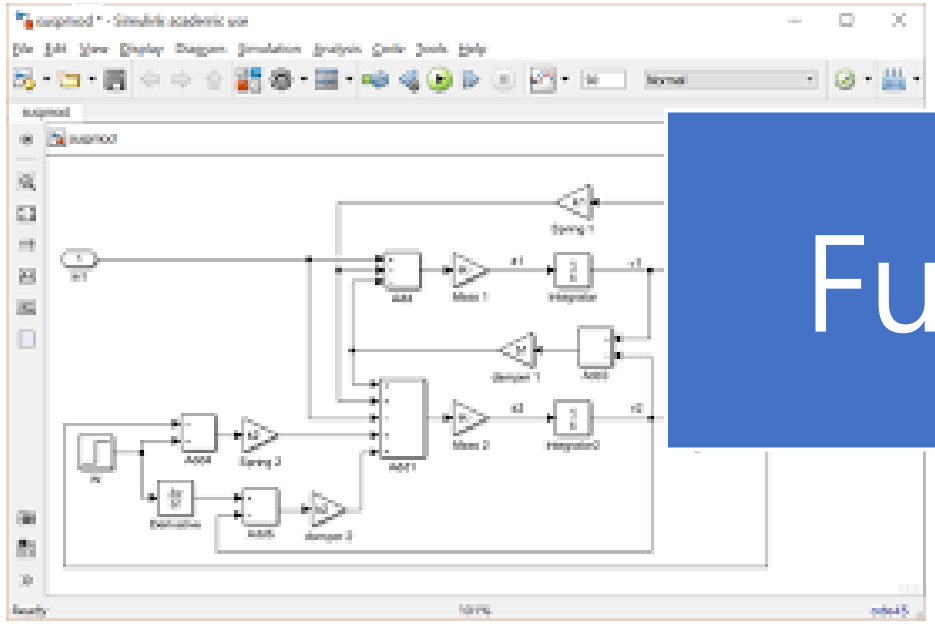
시뮬레이션 기반 위성 소프트웨어 검증



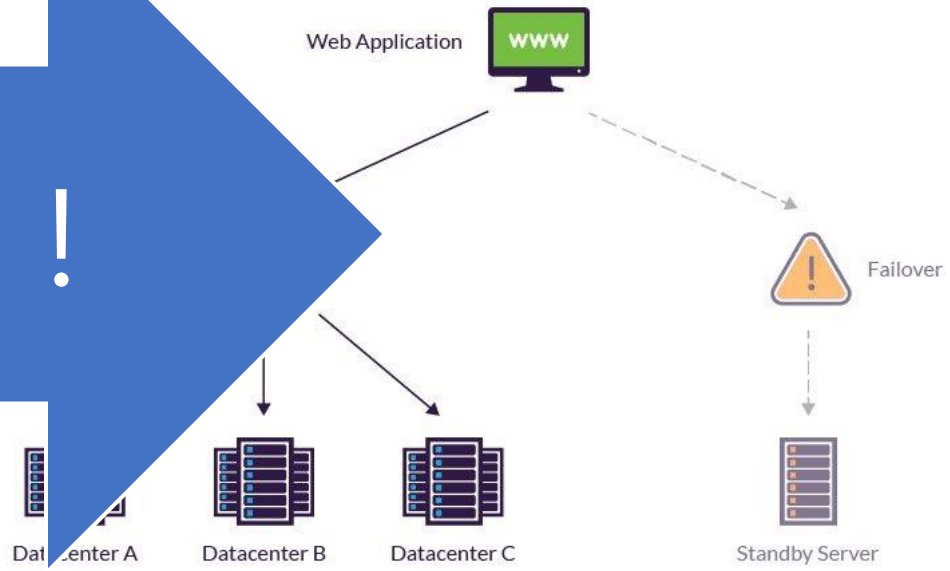
UML 모델 기반 검증 (제임스웹)

Fuzz Testing을 통한 결함 탐지

기존 연구의 한계



Fuzzer !



모델 기반 시뮬레이션 검증

내결함성 소프트웨어 설계 (오류 발생시 사용)

Fuzz Testing을 통한 결함 탐지

왜 Fuzzer인가?

- 기존 방식으로는 찾지 못하는 오류를 발견 가능

- 더 신속하고 효과적으로 결함 탐지 및 수정 가능

- 위성 뿐 아니라 유사한 구조를 가진 다른 시스템 적용 가능

Fuzz Testing을 통한 결함 탐지

Fuzz Testing을 통한 버그 발견 사

Cubesat(초소형 인공위성) 테스트 과정에서 기존 방식으로는 찾지 못했던 12개의 오류를 3일 만에 발견하고 신속하게 수정 가능했음.

TABLE 1. Characterization of the failures found in the SUCHAI flight software.

ID	Command name	Exit Code	Error type	Where is it being executed?			Criticality	Ease of finding	Ease of fixing	Architecture level			Affected modules	#LOC*		#Funcs.**
				SAT	GND	SIM				ORG	EXP	FIX		+	-	
#4	fp_del_cmd_unix	-6	SS				4	3	4	D	A	D	data_storage.c data_storage.h cmdFP.c repoData.c cmdCOM.c	256	119	10
#5	tm_send_status	-6	FA				5	2	3	A	A	A	cmdCOM.h cmdTM.c taskCommunications.c	72	36	3
#6	obc_set_tle	-11	SF				4	3	1	A	A	A	cmdOBC.c	1	1	1
#7	drp_set_deployed	-11	NP				4	2	1	A	A	A	cmdDRP.c	5	8	1
#8	com_send_tc	-6	SS				3	5	5	A	A	A	cmdCOM.c	1	1	1
#9	fp_del_cmd	-11	NP				5	2	1	A	A	A	cmdFP.c	16	18	1
#10	fp_del_cmd_unix	-11	NP				4	1	1	A	A	A	cmdFP.c	9	11	1
#11	fp_set_cmd_dt	-6	SS				4	3	3	D	A	D	data_storage.c globals.h	4	3	1
#12	fp_test_params	-11	SF				1	2	1	A	A	A	cmdFP.c	5	7	1
#13	fp_set_cmd_unix	-11	SF				4	2	1	A	A	A	cmdFP.c	10	11	1
#14	fp_set_cmd_dt	-11	SF				4	2	1	A	A	A	cmdFP.c	10	12	1
#15	fp_set_cmd	-11	SF				4	1	1	A	A	A	cmdFP.c	18	20	1

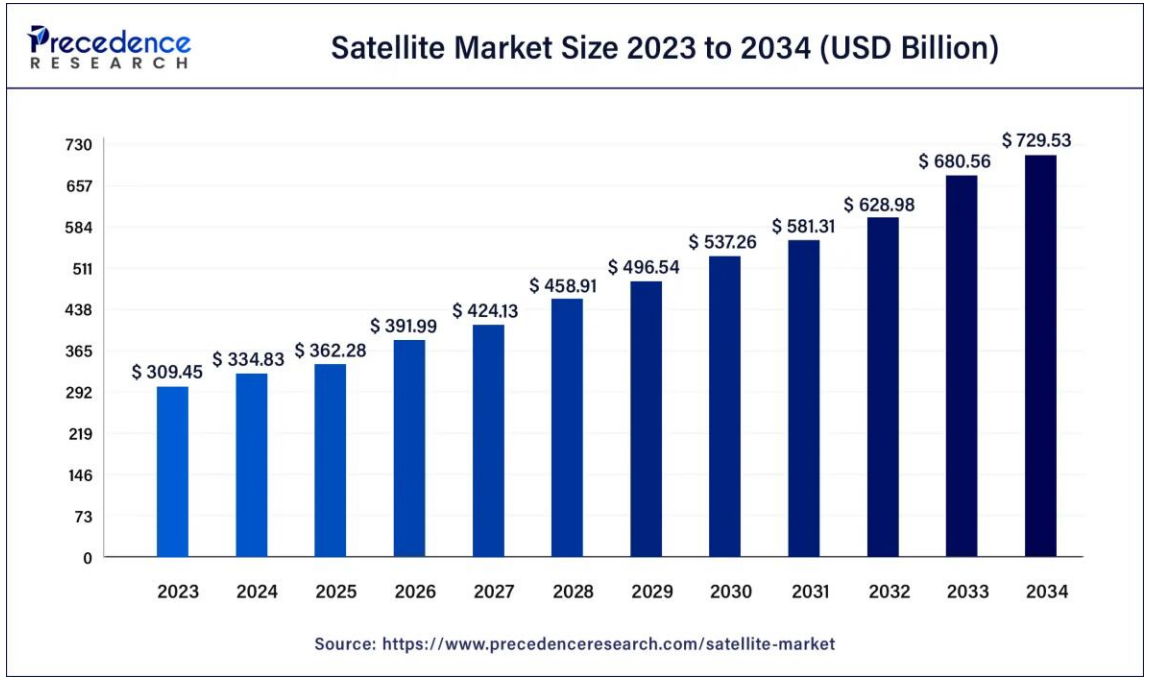
(*) # of code lines to fix de bugs
(**) # of modified functions to fix the bug

출처: Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software for Agile Mission Development

Fuzz Testing을 통한 결함 탐지

연구 목적

미래 7대 산업에 포함될 만큼 중요한 우주 항공 분야에서, Fuzzer를 이용한 위성 검증에 대한 연구 비중이 적음. 본 연구는 Fuzz Testing을 통해 위성 SW의 취약점을 효과적으로 식별하고 이에 대한 해결책을 제시하려는 목표를 가지고 있음.



Fuzz Testing을 통한 결함 탐지

연구 기대 결과

- NASA와 ESA가 제공하는 오픈 소스 위성 소프트웨어들을 수집, 분석.
- 현존 Fuzzer 도구들 적용하여 테스트
- 버그(결함) 탐지
- 개선점 파악

위성 결함 탐지의 중요성

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

위성 결함 탐지의 중요성

관련 연구 요

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 테스팅 완전성을 향상시켰다.	Fuzz Testing을 통한 버그 발견 사례

Thank You