

# Project Design Brief

Project Name	차세대 위성통신 보안 시뮬레이터
-----------------	-------------------

13 조

202002561 조영민

202002546 임우진

202002493 박민서

지도교수: 장진수 교수님

# Document Revision History

---

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2023/03/14	팀원 전체의 의견 수렴과 개요서 작성	임우진

# Table of Contents

---

1. 프로젝트 주제 이름 .....	5
2. 대상 이해당사자 (STAKEHOLDER) .....	5
3. 이해당사자의 고충(PAIN POINT) 또는 니즈(NEEDS) .....	6
4. 이해당사자의 이유 .....	6
5. 프로젝트 수행자의 의도 .....	7
6. 탐구 내용 및 기대 결과 .....	8
7. 프로젝트 관련 학습 계획 .....	9
8. 프로젝트 관련 현장방문 / 인터뷰 / 관찰 계획 .....	9

# List of Figure

---

그림 목차 항목을 찾을 수 없습니다.

## 1. 프로젝트 주제 이름

"차세대 위성통신 보안 시뮬레이터"

(Next Generation Satellite Communication Security Simulator)

## 2. 대상 이해당사자 (stakeholder)

이해당사자	역할 및 참여 목적
위성 운영사	위성 시스템 보안성 시뮬레이션 및 원격 패치 체계 테스트
국방 기관	군사용 위성통신의 제밍/스푸핑 공격 시뮬레이션 및 대응 훈련
통신 서비스 사업자	6G-위성 통신 연동 서비스 시뮬레이션
연구기관	위성 통신 프로토콜 및 보안 알고리즘 성능 검증
교육기관	위성 통신 보안 교육 및 실습 환경 제공

### 3. 이해당사자의 고통(pain point) 또는 니즈(needs)

#### 1. 기존 시뮬레이터 한계:

- 채널 손상(전파 지연, 도플러 효과) 미반영으로 실제 환경 대비 신뢰도 낮음
- 실시간 위성-지상국 통신 시뮬레이션과 보안 취약점 테스트 환경 부재

#### 2. 보안 시뮬레이션 요구:

- 위성-지상국 링크 스푸핑, 재밍 등 다양한 공격 시나리오 시뮬레이션 필요
- 암호화 키 관리 및 갱신 프로세스 테스트 환경 부족

#### 3. 비용 및 접근성 문제:

- 실제 위성 환경 테스트의 높은 비용과 접근성 제한
- 위성 하드웨어 의존 없이 소프트웨어로 다양한 시나리오 검증 필요

### 4. 이해당사자의 이유

#### • 위성 운영사:

- 실제 발사 전 다양한 보안 시나리오 시뮬레이션으로 위험 최소화
- 지상국-위성 간 키 교환 및 패치 프로세스의 안전성 사전 검증 필요

#### • 국방 기관:

- GPS 스푸핑 및 통신 재밍 공격 시뮬레이션을 통한 대응책 개발
- 실제와 유사한 위성 통신 환경에서 운용자 훈련 필요

#### • 연구기관:

- 다양한 암호화 알고리즘 및 프로토콜의 위성 환경 적합성 연구
- 위성 네트워크 보안 기술 개발 및 검증 환경 필요

## 5. 프로젝트 수행자의 의도

### 1. 고정밀 위성 통신 환경 시뮬레이션:

- GNU Radio 와 Gr-Leo 기반 LEO 위성 통신 채널 모델링
- HackRF 2 대를 활용한 이중 주파수 분할 모드 실제 RF 신호 시뮬레이션
- 도플러 효과, 경로 손실, 대기 감쇠 등 우주 환경 요소 실시간 모델링

### 2. 통합 보안 시뮬레이션 환경:

- 위성-지상국 간 키 교환 및 OTAR 프로토콜 시뮬레이션
- 다양한 공격 벡터(재밍, 스푸핑, 중간자 공격 등) 시뮬레이션 모듈
- ARM TrustZone 기반 TEE 보안 환경 시뮬레이션 (QEMU 가상화)

### 3. NASA 표준 기반 소프트웨어 시뮬레이션:

- NASA cFS(Core Flight System) 및 Ground System 통합 시뮬레이션
- CCSDS 표준 준수 통신 프로토콜 시뮬레이션
- 실제 위성 임무 시나리오 기반 시뮬레이션 프로파일

## 6. 탐구 내용 및 기대 결과

### 탐구 내용

분야	세부 기술	시뮬레이션 접근법
위성 채널 특성 분석	도플러 효과, 경로 손실, 대기/강우 감쇠	Gr-Leo 모듈을 활용한 ITU 표준 기반 채널 모델링 및 시뮬레이션
보안 프로토콜 시뮬레이션	OTAR, 키 교환 메커니 즘, 암호화 성능	QEMU 기반 OP-TEE 환경에서 TEE-REE 통신 시뮬레이션
공격 시나리오 모델링	재밍, 스푸핑, 중간자 공 격, 키 탈취	SDR 기반 공격 패턴 생성 및 영향 시뮬레이 션
위성 버스 시스템 동작	ADCS, EPS, CDHS 간 통 신 및 취약점	NASA cFS 기반 위성 서브시스템 시뮬레이 션 및 취약점 분석

### 기대 결과

#### 1. 시뮬레이터 성능 메트릭:

- 채널 모델링 정확도: 실제 LEO 위성 환경 대비 90% 이상 유사도
- 시뮬레이션 처리 성능: 최대 10 개 동시 위성 노드 시뮬레이션
- 암호화/복호화 성능: 실제 환경 대비 1.2 배 이내 처리 시간
- 키 교환 시뮬레이션: BER  $10^{-6}$  환경에서 85% 이상 패킷 복호화 성공률

#### 2. 검증된 시뮬레이션 모델:

- ITU 권고안 준수 위성 채널 모델 라이브러리
- CCSDS 355.0-B-2 호환 보안 프로토콜 시뮬레이션 모듈
- 20 가지 이상의 표준화된 공격 시나리오 템플릿

#### 3. 시뮬레이터 활용 성과:

- 위성 통신 보안 취약점 사전 발견 및 대응책 검증
- 키 교환 프로토콜 성능 최적화 데이터
- 운영자 대응 훈련 효과 측정 지표



## 7. 프로젝트 관련 학습 계획

학습할 내용	기간	역할 분담
GNU Radio 프로그래밍, HackRF 인터페이스	3월	조원 전체
CCSDS 표준, NASA cFS 아키텍처	3월	조원 전체
TEE 시뮬레이션, 암호화 알고리즘	4월	조원 전체
위성 채널 특성, 도플러 효과, 경로 손실	4월	조원 전체

## 8. 프로젝트 관련 현장방문 / 인터뷰 / 관찰 계획

조사할 내용	기간	역할 분담
위성 지상국 운영자 및 엔지니어	미정	미정
위성 보안/ 우주기상 전문가	미정	미정
실제 위성 신호 모니터링	4월-5월	조원 전체