Risk Assessment

Mission Type: Communication Satellite

# Main Threats Overview

|  |  |
| --- | --- |
| **Threat** | **Probability** |
| Data Corruption | High |
| Physical/Logical Attack | Medium |
| Interception/Eavesdropping | High |
| Jamming | Very High |
| Denial-of-Service | High |
| Masquerade/Spoofing | Medium |
| Replay | Low |
| Software Threats | Medium |
| Unauthorized Access/Hijacking | High |
| Tainted hardware components | Medium |
| Supply Chain | High |

# Detailed Threat Analysis

## Data Corruption

Loss/modification of user traffic  
Routing errors

### Asset

Link  
User

### Security Controls for Data Corruption

End-to-end encryption  
Forward error correction  
Secure checksums

## Physical/Logical Attack

Satellite takeover  
Ground station compromise

### Asset

Ground  
Space

### Security Controls for Physical/Logical Attack

Tamper-proof hardware  
Secure boot lander  
Zero-trust architecture for ground segments

## Interception/Eavesdropping

Theft of sensitive communications

### Asset

Link

### Security Controls for Interception/Eavesdropping

Over-the-air encryption  
Frequency hopping  
Low-probability-of-intercept waveforms

## Jamming

Disruption of user links (voice/data)

### Asset

Ground  
Space

### Security Controls for Jamming

Anti-jamming antennas  
Spread spectrum  
Dynamic power/frequency adjustment

## Denial-of-Service

Overload of satellite/gateway  
Service disruption

### Asset

Ground  
Space

### Security Controls for Denial-of-Service

Traffic shaping  
Rate limiting  
Redundant gateways  
Onboard DoS detection

## Masquerade/Spoofing

Fake control commands  
Rogue base stations

### Asset

Ground  
Space  
Link

### Security Controls for Masquerade/Spoofing

Strong authentication  
geolocation validation  
Beacon signals for legitimacy checks

## Replay

Reuse of old commands

### Asset

Ground  
Space  
Link

### Security Controls for Replay

Timestamped commands  
One-time tokens  
Cryptographic nonces

## Software Threats

Firmware exploits  
Malware in ground systems

### Asset

Ground  
Space

### Security Controls for Software Threats

Air-gapped testing  
Runtime integrity checks  
Secure Over-the-Air updates

## Unauthorized Access/Hijacking

Theft of bandwidth  
Satellite hijacking

### Asset

Ground  
Space  
Link

### Security Controls for Unauthorized Access/Hijacking

Hardware-based access control (smart cards)  
Multi-factor authentication  
Command link encryption

## Tainted hardware components

Backdoors in modems/router  
Signal manipulation

### Asset

Ground  
Space

### Security Controls for Tainted hardware components

Trusted suppliers  
Hardware attestation  
Supply-chain audits

## Supply Chain

Counterfeit transponders  
Malicious firmware

### Asset

Ground  
Space

### Security Controls for Supply Chain

Vendor vetting  
Component fingerprinting  
Secure boot with signed firmware