Risk Assessment

Mission Type: Navigation Satellite

# Main Threats Overview

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

# Detailed Threat Analysis

## Data Corruption

Erroneus positioning/timing  
System drift

### Asset

Link  
User

### Security Controls for Data Corruption

Cryptographic authentication  
Integrity checks  
Redundant atomic clocks

## Physical/Logical Attack

Satellite takeover  
Ground station compromise

### Asset

Ground  
Space

### Security Controls for Physical/Logical Attack

Tamper-resistant hardware  
Secure boot loaders  
Zero-trust architecture for ground segments

## Interception/Eavesdropping

Intelligence gathering  
Spoofing preparation

### Asset

Link  
User

### Security Controls for Interception/Eavesdropping

Encrypted signals  
Ant-eavesdropping waveforms  
Frequency hopping

## Jamming

Disruption services

### Asset

Ground  
Space  
Link  
User

### Security Controls for Jamming

Anti-jamming antennas  
High-power signals  
Alternative sources

## Denial-of-Service

Overload of control segment  
Service outage

### Asset

Ground  
Space

### Security Controls for Denial-of-Service

Traffic filtering  
Rate limiting  
Ground station redundancy  
Onboard DoS detection

## Masquerade/Spoofing

Incorrect positioning

### Asset

Ground  
Space  
Link  
User

### Security Controls for Masquerade/Spoofing

Signal authentication  
Cross-checking with other constellation

## Replay

Timing/navigation errors

### Asset

Ground  
Space  
Link

### Security Controls for Replay

Timestamped signals  
Cryptographic nonces  
Rapid key rotation

## Software Threats

Exploits in timing algorithms  
Firmware hijacking

### Asset

Ground  
Space

### Security Controls for Software Threats

Secure coding  
Runtime monitoring  
Air-gapped testing

## Unauthorized Access/Hijacking

Unauthorized command upload  
Key theft

### Asset

Ground  
Space  
Link

### Security Controls for Unauthorized Access/Hijacking

Multi-factor authentication  
Hardware security modules  
Secure key distribution

## Tainted hardware components

Backdoors in atomic clocks / signal generators

### Asset

Ground  
Space

### Security Controls for Tainted hardware components

Trusted suppliers  
Radiation-hardened components  
Hardware attestation

## Supply Chain

Compromised oscillators / encryption chips

### Asset

Ground  
Space

### Security Controls for Supply Chain

Vendor vetting  
Component testing  
Secure boot with signed firmware