Risk Assessment

Mission Type: Earth Observation Satellite

# Main Threats Overview

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

# Detailed Threat Analysis

## Data Corruption

Modification of mission / science data  
System instability

### Asset

Ground  
Link

### Security Controls for Data Corruption

Data integrity (hashing, checksum, digital signatures)  
Error-correction codes (ECC)  
Resilient onboard storage

## Physical/Logical Attack

Loss of control  
Data theft  
Satellite hijacking

### Asset

Ground  
Space

### Security Controls for Physical/Logical Attack

Secure facility access (guards, biometrics)  
Secure boot  
Firmware validation  
Intrusion detection Systems

## Interception/Eavesdropping

Theft of sensitive Earth observation data

### Asset

Link

### Security Controls for Interception/Eavesdropping

Encryption for data at rest/in transit  
Secure key management  
Protected downlink (frequency hopping, low probability of intercept)

## Jamming

Loss of telemetry/command link  
Disruption of data downlink

### Asset

Ground  
Space

### Security Controls for Jamming

Spread spectrum  
Multiple ground stations  
Adaptive power control  
Anti-jamming antennas

## Denial-of-Service

Overload of ground station/satellite  
Loss of mission operations

### Asset

Ground  
Space

### Security Controls for Denial-of-Service

Firewall  
Rate limiting  
Redundant network paths  
Onboard DoS detection  
Priority-based command scheduling

## Masquerade/Spoofing

Unauthorized command injection  
False data injection

### Asset

Ground  
Space  
Link

### Security Controls for Masquerade/Spoofing

Strong authentication  
Command source validation  
Secure time-synchronization

## Replay

Execution of old commands  
System instability

### Asset

Ground  
Space  
Link

### Security Controls for Replay

Command counters  
Timestamps  
One-time tokens  
Secure sequence numbering

## Software Threats

Malware  
Zero-day exploits  
System compromise

### Asset

Ground  
Space

### Security Controls for Software Threats

Secure coding practices  
Static/dynamic code analysis  
Runtime monitoring  
Sandboxing critical functions

## Unauthorized Access/Hijacking

Theft of mission data  
Satellite takeover

### Asset

Ground  
Space  
Link

### Security Controls for Unauthorized Access/Hijacking

Multi-factor authentication  
Role-based access control  
Hardware security modules  
Secure command encryption

## Tainted hardware components

Backdoors  
Systems failure  
Data leakage

### Asset

Ground  
Space

### Security Controls for Tainted hardware components

Trusted suppliers  
Hardware attestation  
Secure boot  
Firmware signing  
Hardware Trojan detection

## Supply Chain

Counterfeit parts  
Malicious implants  
Delays

### Asset

Ground  
Space

### Security Controls for Supply Chain

Vendor vetting  
Chain-of-custody tracking  
Component testing  
Secure procurement policies