Risk Assessment

Mission Type: Science Mission

# Main Threats Overview

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

# Detailed Threat Analysis

## Data Corruption

Loss/modification of scientific data  
Calibration errors

### Asset

Ground  
Link

### Security Controls for Data Corruption

Checksums  
Error correction  
Onboard storage redundancy  
End-to-end validation (digital signatures)

## Physical/Logical Attack

Unauthorized access to instruments  
Mission sabotage

### Asset

Ground  
Space

### Security Controls for Physical/Logical Attack

Secure boot lander  
Firmware signing  
Hardware security modules  
Minimal attack surface

## Interception/Eavesdropping

Theft of proprietary science data

### Asset

Link

### Security Controls for Interception/Eavesdropping

Encrypted downlinks  
Frequency agility  
Delayed data release

## Jamming

Loss of telemetry/command link  
Disruption of data downlink

### Asset

Ground  
Space  
Link

### Security Controls for Jamming

Multiple ground stations  
Adaptive signal processing  
Robust error correction

## Denial-of-Service

Overload of ground station/satellite  
Loss of science operations

### Asset

Ground  
Space

### Security Controls for Denial-of-Service

Traffic filtering at ground stations  
Onboard command queuing  
Priority-based data transmission

## Masquerade/Spoofing

Fake commands

### Asset

Ground  
Space  
Link

### Security Controls for Masquerade/Spoofing

Command counters  
Timestamps  
One-time tokens  
Secure sequence numbering

## Replay

Execution of old commands  
Resetting instruments

### Asset

Ground  
Space  
Link

### Security Controls for Replay

Command counters  
Timestamps  
One-time tokens  
Secure sequence numbering

## Software Threats

Exploits in instrument control  
Data processing flaws

### Asset

Ground  
Space

### Security Controls for Software Threats

IV&V (Independent Verification & Validation)  
Sandboxing of critical functions  
Runtime anomaly detection

## Unauthorized Access/Hijacking

Theft of mission data  
Unauthorized instrument control

### Asset

Ground  
Space  
Link

### Security Controls for Unauthorized Access/Hijacking

Role-based access control  
Secure command encryption  
Hardware-enforced isolation

## Tainted hardware components

Compromised sensor/processors  
Data manipulation

### Asset

Ground  
Space

### Security Controls for Tainted hardware components

Trusted suppliers  
Component testing  
Radiation-hardened  
Tamper-proof designs  
Redundant cross-checks

## Supply Chain

Counterfeit parts  
Malicious implants in instruments

### Asset

Ground  
Space

### Security Controls for Supply Chain

Secure procurement  
Chain-of-custody tracking  
Destructive/non destructive testing  
Vendor vetting