Risk Assessment

Mission Type: On-Orbit Service

# Main Threats Overview

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

# Detailed Threat Analysis

## Data Corruption

Erroneus commands  
Collision/damage

### Asset

Ground  
Space

### Security Controls for Data Corruption

Secure checksum  
Real-time command validation  
Hardware redundancy

## Physical/Logical Attack

Unauthorized control of servicer  
Sabotage/theft

### Asset

Ground  
Space

### Security Controls for Physical/Logical Attack

Secure docking protocols  
Tamper-proof robotics  
Zero-trust communication links

## Interception/Eavesdropping

Theft of proprietary servicing tech

### Asset

Ground  
Space  
Link

### Security Controls for Interception/Eavesdropping

Encrypted telemetry/commands  
Frequency-hopping for critical operations

## Jamming

Loss of control during proximity operations  
Collision risk

### Asset

Ground  
Space  
Link

### Security Controls for Jamming

Redundant communications  
Autonomous collision avoidance  
Anti-jamming waveforms

## Denial-of-Service

Disruption of servicing operations

### Asset

Ground  
Space

### Security Controls for Denial-of-Service

Priority-based bandwidth allocation  
Onboard contingency plans  
Ground-segment redundancy

## Masquerade/Spoofing

Servicer hijacking

### Asset

Ground  
Space  
Link

### Security Controls for Masquerade/Spoofing

Mutual authentication  
Cross-verification with ground stations  
Optical navigation as primary  
Cryptographic relative GPS

## Replay

Unintended maneuvers

### Asset

Ground  
Space  
Link

### Security Controls for Replay

Timestamped/nonce-based commands  
One-time tokens for critical operations

## Software Threats

Irregular behavior

### Asset

Ground  
Space

### Security Controls for Software Threats

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

## Unauthorized Access/Hijacking

Theft of orbital assets

### Asset

Ground  
Space  
Link

### Security Controls for Unauthorized Access/Hijacking

Hardware-enforced access control  
Hardware-enforced motion limits  
Secure docking “handshake”  
Cryptographic authentication

## Tainted hardware components

Mission sabotage

### Asset

Ground  
Space

### Security Controls for Tainted hardware components

Trusted suppliers  
Onboard hardware attestations  
Dual-channel actuators  
Mechanical interlocks  
Multi-sensor validation

## Supply Chain

Counterfeit parts in critical systems

### Asset

Ground  
Space

### Security Controls for Supply Chain

Secure procurement  
Pre-launch destructive testing  
Component serialization