International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

# Zero Trust for LEO Satellite Command Systems

**Vismit Rakhecha**

Independent Researcher, India
Email: *rvismit[at]gmail.com*

**Abstract:** ***This paper proposes Mission-Zero, a Zero Trust security architecture designed for Low Earth Orbit satellite command systems. Traditional satellite security models rely heavily on trusted ground infrastructure and perimeter-based defenses, which are increasingly insufficient against modern cyber threats such as RF spoofing, command replay attacks, and ground system compromise. The proposed framework introduces continuous verification across the entire command chain, including operator authentication, command validation, ground station protection, secure RF communication, and onboard satellite verification. By applying Zero Trust principles to satellite command and control infrastructure, the architecture improves resilience against unauthorized command injection and infrastructure compromise while maintaining lightweight operational overhead suitable for LEO missions.***

**Keywords:** LEO Satellite, Zero Trust, Zero Trust Architecture, Ground Station, Cyber Security

## 1. Introduction

Satellites in Low Earth Orbit are no longer just scientific tools; they have become critical infrastructure. From real-time disaster alerts and border monitoring to climate data and secure communications, ISRO's LEO fleet (EOS-09, NISAR, and the growing constellation) keeps India's eyes on the planet 24×7. But while the hardware is cutting-edge, the security model protecting them is still stuck in the 1990s.

Traditional "perimeter defence assumes the ground station is always trusted and the RF link is always safe. That assumption died years ago. Today, adversaries spoof uplink signals during 8-minute visibility windows, replay captured commands hours later, jam S-band links from border regions, and even steal ground-operator credentials. A single successful injection can trigger rogue operation, corrupt payload data, or force the satellite into permanent safe-hold.

"We needed a different approach" Mission-Zero replaces the old "trust but verify" castle wall with genuine Zero Trust continuous, real-time verification of every single command against the satellite's live orbital state, mission phase, and signal reality.

## 2. Threat Modelling for LEO Satellite Systems

These threats are not purely theoretical; similar vulnerabilities have been observed in satellite communication environments worldwide. Here's what LEO fleet is actually facing every single day:

a) ***RF Spoofing***: Bad actors pretend to be legitimate ground stations during short visibility windows. Using commercially available software-defined radios (SDRs) available on the open market, attackers can transmit from anywhere in line-of-sight, making the spoofed uplink look identical to an official ISRO station.
b) ***Command Replay***: They record a valid packet and blast it back later. A perfectly legitimate command captured during one overhead pass can be replayed hours or even days later from a completely different longitude, bypassing simple sequence numbers or timestamps that most legacy systems still rely on.
c) ***Identity Drift***: Ground credentials get stolen and slowly abused. Once an operator token, certificate, or account is compromised (through phishing, keyloggers, or supply-chain attacks), adversaries can issue commands gradually over multiple passes without triggering immediate alerts — the classic "low-and-slow" approach.
d) ***Signal Flooding***: High-power jammers force the satellite into safe-hold mode. Coordinated jamming from border regions, ships, or even truck-mounted systems can drop the signal-to-noise ratio by 25–30 dB in seconds, blinding the S-band receiver and creating the perfect window for follow-on injection attacks while the satellite is forced into emergency "Safe-Hold."

## 3. Real World Threat Landscape

These threats are not purely theoretical; similar vulnerabilities have been observed in satellite communication environments worldwide. Here's what LEO fleet is actually facing every single day:

**Table I**

| Stride Category | Threat | Impact on LEO Satellite Systems | Stride Category |
|---|---|---|---|
| Spoofing | RF command spoofing | Fake commands transmitted to the spacecraft through uplink frequencies | Spoofing |
| Spoofing | Ground station impersonation | Rogue ground stations attempt unauthorized command uplinks | Spoofing |
| Spoofing | Credential compromise | Attackers impersonate mission operators to issue commands | Spoofing |
| Tampering | Command injection | Orbital configuration commands altered in transit | Tampering |
| Tampering | Telemetry manipulation | False spacecraft health data transmitted to ground control | Tampering |
| Tampering | Firmware modification | Malicious firmware uploaded leading to persistent spacecraft control | Tampering |

| | | | |
|---|---|---|---|
| Repudiation | Command log tampering | Adversaries erase or modify command execution records | Repudiation |
| Repudiation | Ground system audit removal | Intrusion evidence removed from mission control infrastructure | Repudiation |
| Information Disclosure | Telemetry interception | Adversaries monitor spacecraft orbit, subsystem health, and operations | Information Disclosure |
| Information Disclosure | Payload data capture | Scientific or imaging data intercepted during downlink | Information Disclosure |
| Denial of Service | RF jamming | Satellite unable to receive legitimate command uplinks | Denial of Service |
| Denial of Service | Ground station attack | Mission control infrastructure disrupted or taken offline | Denial of Service |
| Elevation of Privilege | Mission control compromise | Unauthorized users gain satellite command authority | Elevation of Privilege |
| Elevation of Privilege | Firmware exploitation | Vulnerabilities used to gain persistent access to onboard systems | Elevation of Privilege |

## 4. Zero Trust Security Principles

Zero Trust is a modern cybersecurity paradigm that assumes no system component is inherently trustworthy. Unlike traditional perimeter-based security models that rely on trusted internal networks, Zero Trust architectures operate under the assumption that every interaction must be verified regardless of its origin. This approach is particularly relevant for satellite systems where communications occur over open radio frequencies and ground infrastructure may be geographically distributed.

Zero Trust operates on three core assumptions:

1) Never trust, always verify
2) Assume breach
3) Continuously validate identity and system integrity

For satellite systems, this means:

1) Verifying every command
2) Validating every operator identity
3) Continuously monitoring spacecraft telemetry

## 5. Zero Trust Architecture Components for LEO Satellite Command Systems

The proposed Mission-Zero framework introduces multiple security layers across both the ground segment and space segment. Each layer performs a specific trust validation function before commands are transmitted or executed.

**Table III**

| Layer | Description |
|---|---|
| Operator Identity Layer | Ensures that every mission operator or automated system interacting with the satellite command infrastructure is strongly authenticated using mechanisms such as multi-factor authentication (MFA), hardware tokens, and role-based identity verification. |
| Zero Trust Policy Engine | Acts as the central decision authority that evaluates whether a requested command is permitted. It validates the operator's role, mission context, command type, and predefined operational policies before approving execution. |
| Command Security Gateway | Serves as the enforcement point for all satellite commands. It validates command structure, applies cryptographic signing, enforces rate limits, and prevents unauthorized or malformed commands from reaching the ground station. |
| Ground Station Security Layer | Protects the terrestrial infrastructure responsible for transmitting commands. This layer ensures mutual authentication between mission control and ground stations, implements network segmentation, and protects uplink systems from unauthorized access. |
| RF Communication Protection | Secures the radio frequency communication channel between ground stations and satellites using encryption, authentication, replay protection, and signal validation mechanisms to prevent spoofing or interception. |
| Onboard Satellite Verification | Provides the final security checkpoint within the spacecraft. The onboard flight computer verifies command signatures, validates execution policies, and rejects unauthorized instructions before activating any subsystem operations. |
| Telemetry Monitoring and Analytics | Continuously analyzes spacecraft telemetry to detect anomalies, suspicious commands, or abnormal subsystem behavior. This layer enables early detection of cyber incidents and supports mission security monitoring. |

## 6. Secure Command Flow in a Zero Trust Satellite Architecture


**Figure 1**

## 7. Satellite Onboard Security Controls

Unlike terrestrial systems, satellites operate in an environment where physical access is extremely limited once deployed. As a result, onboard security mechanisms must provide autonomous protection against malicious commands, software tampering, and abnormal system behavior. In Low Earth Orbit (LEO) missions, spacecraft communicate over open radio frequency channels and rely heavily on ground infrastructure, which increases exposure to potential cyber threats.

To mitigate these risks, modern satellite architectures implement a set of onboard security controls designed to ensure **firmware integrity, command authenticity, subsystem isolation, and operational resilience**. These mechanisms allow the spacecraft to independently validate commands, protect critical subsystems, and maintain safe operation even if communication channels or ground systems are compromised. The following controls represent key security measures that can be integrated into LEO satellite platforms.

**Table IIIII**

| Security Control | Description | Security Benefit |
|---|---|---|
| Secure Boot | Ensures the spacecraft boots only trusted firmware verified through cryptographic signatures. | Prevents execution of malicious or modified flight software. |
| Firmware Integrity Verification | Periodic validation of onboard software using cryptographic hashes or signatures. | Detects unauthorized firmware modification. |
| Command Authentication | All received commands must include valid digital signatures before execution. | Prevents spoofed or injected commands. |
| Command Whitelisting | Only predefined and approved command types can be executed by the spacecraft. | Blocks unauthorized or dangerous commands. |
| Replay Protection | Commands include timestamps or sequence numbers to prevent reuse of captured command frames. | Mitigates replay attacks on the RF uplink. |
| Subsystem Isolation | Critical subsystems such as propulsion, power, and payload are logically separated. | Limits impact of compromised components. |
| Onboard Access Control | Internal flight software enforces role-based permissions for subsystem operations. | Prevents unauthorized internal command execution. |
| Secure Telemetry Generation | Telemetry data is signed or protected against tampering before transmission. | Ensures integrity of spacecraft status information. |
| Cryptographic Key Storage | Encryption and authentication keys are stored in secure hardware modules. | Protects keys from extraction or tampering. |
| Watchdog and Fault Monitoring | Hardware watchdog timers monitor system behavior and trigger recovery mechanisms. | Prevents persistent control by malicious software. |
| Safe Mode Protection | Satellite can enter a protected operational mode when abnormal behavior is detected. | Protects mission during suspected cyber or system failures. |
| Command Rate Limiting | Limits number of commands processed within a specific time window. | Prevents command flooding attacks. |
| Intrusion Detection Logic | Onboard algorithms detect abnormal command patterns or | Enables early detection of cyber anomalies. |

| | | |
|---|---|---|
| | subsystem activity. | |
| Secure Time Synchronization | Ensures spacecraft maintains trusted time references for command validation. | Prevents attacks that manipulate timing-based operations. |

## 8. Threat Scenario Evaluation

In the Mission-Zero architecture, even if an attacker successfully transmits a spoofed RF command signal, the spacecraft will reject the command because it lacks a valid digital signature and does not satisfy the Zero Trust policy conditions. This additional verification layer significantly reduces the risk of unauthorized command execution.

Consider a malicious actor attempting to send a spoofed orbital maneuver command.

Traditional Architecture
a) Attacker spoofs RF signal
b) Ground station receives command
c) Satellite executes maneuver

**Result:** Potential loss of mission control.

Mission-Zero Architecture
a) RF command received
b) Satellite verifies signature
c) Command rejected due to invalid identity

**Result:** Attack blocked.

## 9. Benefits of Zero Trust for LEO Missions

The adoption of a Zero Trust security model significantly enhances the protection of satellite command and control systems operating in Low Earth Orbit. Unlike traditional security architectures that rely on trusted networks or perimeter defences, Zero Trust enforces strict verification for every user, device, and communication channel involved in mission operations. This approach is particularly important for LEO satellites, where command links operate over open radio frequencies and mission infrastructure may be distributed across multiple ground stations and networks.

By enforcing identity verification, command authentication, and continuous monitoring, Zero Trust architectures reduce the likelihood of unauthorized command execution, signal manipulation, and infrastructure compromise. The following table highlights key areas where Zero Trust improves the overall security posture of LEO satellite missions.

**Table IV**

| Security Area | Improvement |
|---|---|
| Command Authentication | Prevents spoofed uplink commands by requiring cryptographic verification before execution. |
| Ground Infrastructure Security | Limits lateral movement within mission control networks through strict access control and segmentation. |
| RF Link Security | Reduces the risk of signal injection or interception through encrypted and authenticated communication channels. |
| Operational Monitoring | Enables early detection of anomalies by continuously analyzing command activity and telemetry data. |
| Constellation Protection | Prevents compromise from spreading across satellites in a constellation through identity and policy enforcement. |

## 10. Implementation Roadmap

Implementing a Zero Trust architecture for LEO satellite systems requires a phased approach that integrates security controls across mission control infrastructure, communication channels, and spacecraft subsystems. Rather than attempting a full architectural transformation at once, satellite operators can progressively introduce Zero Trust capabilities in stages that align with operational priorities and system maturity.

The following roadmap outlines a practical sequence for adopting Zero Trust security within satellite command and control environments.

**Phase 1- Identity Security**
The first step focuses on strengthening operator authentication and access control within mission control systems. This phase ensures that only verified personnel can interact with satellite command infrastructure.

**Key measures include:**
- Implementation of multi-factor authentication (MFA) for mission operators
- Deployment of hardware authentication keys or smart cards
- Enforcement of role-based access control (RBAC) to restrict command privileges

These controls establish a strong identity foundation for the Zero Trust architecture.

**Phase 2 - Command Security**
The second phase secures the command generation and validation pipeline. Commands must be authenticated and protected before transmission to prevent spoofing or manipulation.

**Key measures include:**
- Cryptographic signing of satellite commands
- Deployment of secure command gateways for validation and enforcement
- Implementation of replay protection mechanisms such as timestamps and sequence numbers

This phase ensures that only verified and authorized commands are transmitted to spacecraft.

**Phase 3- Ground Network Security**
The third phase focuses on securing the ground segment infrastructure that supports satellite operations. Ground

networks must be protected against unauthorized access and lateral movement.

**Key measures include:**
- Network segmentation within mission control environments
- Deployment of Zero Trust access gateways for ground systems
- Continuous monitoring and logging of operator activity and command traffic

These controls reduce the risk of infrastructure compromise affecting mission operations.

**Phase 4 - Spacecraft Security**
The final phase integrates security mechanisms directly within the spacecraft to ensure autonomous validation of commands and system integrity.

**Key measures include:**
- Secure boot mechanisms to protect flight software integrity
- Onboard command validation modules to authenticate uplink instructions
- Telemetry-based anomaly detection to identify abnormal spacecraft behavior

## 11. Conclusions

The rapid expansion of Low Earth Orbit (LEO) satellite missions has significantly increased the importance of robust cybersecurity measures for space infrastructure. Traditional satellite security models often rely on trusted ground networks and static authentication mechanisms, which are increasingly insufficient in an environment characterized by open radio frequency communications, distributed ground systems, and growing adversarial capabilities.

The proposed framework introduces layered protections across the **operator identity layer, command security gateway, ground infrastructure, RF communication channels, and onboard satellite verification mechanisms**. Additionally, integrating supply chain security and onboard security controls strengthens mission resilience throughout the entire satellite lifecycle.

Adopting Zero Trust principles in satellite operations enables mission operators to reduce the risk of cyber compromise while maintaining operational reliability. As the number of satellites and constellations in LEO continues to grow, implementing such security architectures will become essential for protecting critical space infrastructure and ensuring the long-term sustainability of space operations.

Future research may explore automated anomaly detection, machine learning-based telemetry analysis, and adaptive trust policies for large satellite constellations.

**Acknowledgement**
The author would like to acknowledge the broader **space cybersecurity and satellite operations community** whose research and open technical discussions continue to advance the understanding of cyber risks in space systems. The insights from publicly available research, satellite mission documentation, and cybersecurity frameworks have significantly contributed to shaping the concepts presented in this work.

## References

[1] National Institute of Standards and Technology (NIST), Zero Trust Architecture, NIST Special Publication 800-207, 2020.
[2] European Space Agency (ESA), Space Systems Security Handbook, ESA Security Office, 2021.
[3] NASA Office of the Chief Engineer, NASA Systems Engineering Handbook, NASA SP-2016-6105 Rev2.
[4] CCSDS (Consultative Committee for Space Data Systems), Security Guide for Space Missions, CCSDS 350.1-G-3.
[5] Space ISAC, Space Systems Cybersecurity Framework, Space Information Sharing and Analysis Center, 2022.
[6] National Academies of Sciences, Cybersecurity of Space Systems, Washington, DC, 2020.
[7] MITRE Corporation, ATT&CK Framework for Space Systems, MITRE Research Initiative.
[8] IEEE Aerospace Conference Proceedings, Cybersecurity Challenges in Satellite Communications Systems, IEEE Aerospace Conference.