MediSat: A Secure Delay-Tolerant CubeSat Constellation for Medical Data Relay in Infrastructure-Degraded Environments

Doris Ikezeora †*, Karan Shory †, Prachi Singh †, Jakub Gutowski †, Atef Amar †, Divin Raj Sundararaj, Arathy Rajendran Nair, Abu Sufiyan, Jakub Giembicki, Sena Sezen †, Szymon Kafel, Afiya Bagwan, Mark Trubetskoy

April 30, 2026

Abstract

Reliable transmission of medical data during disasters and in remote regions remains a critical challenge due to damaged, congested, or nonexistent terrestrial communication infrastructure. This paper presents MediSat, a SmallSat-based system concept for secure, delay-tolerant relay of medical data using a constellation of CubeSats operating in low Earth orbit. The proposed architecture employs a store-and-forward networking approach combined with end-to-end encryption, autonomous onboard data handling, and quality-of-service prioritization to enable resilient transmission of time-critical healthcare information between field medical units and centralized healthcare systems.

The system design is developed using a structured systems engineering methodology aligned with ECSS practices and SmallSat constraints, covering mission definition, functional decomposition, subsystem allocation, and interface management. Key technical features include delay-tolerant networking protocols, encrypted data storage and transmission, autonomous scheduling of communication windows, and scalable constellation architecture. Subsystem-level considerations for communications, onboard data handling, power, attitude control, and thermal management are discussed to demonstrate feasibility within CubeSat mass, power, and volume limits.

The paper highlights the applicability of the proposed architecture to disaster response, humanitarian operations, and remote healthcare connectivity, and discusses expected performance, scalability, and verification approaches. MediSat demonstrates how SmallSat constellations can be systematically adapted to support secure, resilient medical communications, extending SmallSat applications beyond conventional Earth observation and Internet-of-Things use cases.

Keywords: *SmallSat Constellation, Delay-Tolerant Networking (DTN), Store-and-Forward Communication, Inter-Satellite Links (ISL), Systems Engineering, Disaster Response, Resilient Communication Networks*

1. INTRODUCTION

Reliable transmission of medical data is a critical enabler for effective healthcare delivery in disaster response and remote environments. However, terrestrial communication infrastructure is often unavailable, damaged, or congested during such scenarios, resulting in delayed or failed transmission of time-critical medical information. This limitation highlights the need for resilient, infrastructure-independent communication systems capable of maintaining service continuity under adverse conditions.

This paper presents MediSat, a SmallSat-based system concept designed to provide secure and delay-tolerant medical data relay through a constellation of CubeSats operating in Low Earth Orbit. The system adopts a store-and-forward communication architecture, enabling asynchronous data exchange between field medical units and centralized healthcare systems, ensuring robustness against intermittent connectivity and disrupted ground infrastructure.

Beyond the system concept itself, this work adopts a structured systems engineering approach aligned with ECSS standards, covering not only system design but also the requirements engineering process that drives the design, ensuring traceability from mission needs to subsystem implementation. A dedicated focus is placed on the derivation, allocation and verification of requirements across the system and subsystem levels, according to iterative baseline practices.

In addition, the paper investigates the verification and validation (V&V) framework required to demonstrate system compliance and mission effectiveness. This includes verification strategies that include analysis, inspection, testing, and review-of-design methods, applied at the mission, system, and subsystem levels to ensure that the MediSat architecture meets functional, performance, and security requirements .

From a technical perspective, MediSat integrates delay-tolerant networking (DTN), end-to-end encryption, autonomous onboard data handling, and quality-of-service prioritization, ensuring that sensitive medical data is securely transmitted and critical information is prioritized under constrained conditions.

This paper therefore contributes not only a novel system architecture, but also a comprehensive engineering framework, demonstrating how requirements engineering, system design, and verification processes are cohesively applied to develop a resilient SmallSat-based medical communication system. MediSat ultimately illustrates how CubeSat constellations can be extended beyond traditional applications to support secure, reliable, and scalable healthcare connectivity.

1.1. Concept of Operations

MediSat works as an independent, encrypted, store-and-forward medical data relay satellite constellation meant for disaster-prone regions (the Ring of Fire as the focus for this study) and locations with inadequate infrastructure. This concept (illustrated in figure 1) is built on a system of systems design framework, which is made up of a space segment comprising set of 54 satellites using prominent data relay constellation configuration and measuring 12U each, a distributed ground segment with mission control and delivery capabilities, and user terminals controlled by medical/humanitarian staff in the field. When in normal operation, medical information is produced from the user terminal; it is encrypted and assigned a priority value, and uploaded to the nearest satellite whenever there is availability during visibility periods, transported and transmitted throughout the satellite network if necessary, and received at the ground node linked to health care facilities or mission operations facilities. A success message is returned through the very same structure to the sender, thus enabling the satellite system to facilitate clinical communication regardless of terrestrial network status.

Intermittent connectivity, ISL, is the key principle behind the system design. The function of each satellite within the system is to be an independent relay node that can validate, store, prioritize, and forward the medical information and also engage in maintenance and recovery activities. Through inter-satellite connections and distributed ground stations, the network will be able to deliver reliable services despite any local disruptions, geometric changes, and space vehicle malfunctions.

*Corresponding author: ikezeoradoris@gmail.com (D. Ikezeora).
†These authors contributed equally to this work.

The base operational data flow is on fig. 1 below.

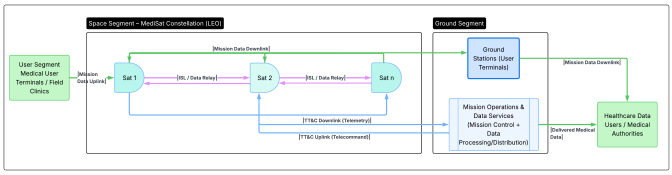

Figure 1. Operational data flow

The operational lifecycle of the MediSat mission is structured into a sequence of different service phases:

- Launch and early orbit operations (LEOP)
- Commissioning and constellation build-up
- Nominal operations
- Safe mode
- End-of-life disposal.

The commissioning phase encompasses a systematic verification of each satellite's core functional capabilities, including onboard data handling ability, power budget positivity, timing synchronisation with the mission reference clock, inter-link and ground communications effectiveness, and cryptographic readiness for secure medical data transmission.

During nominal operations, constellation-level health and scheduling oversight is maintained by the Mission Operations Centre, while routine store-and-forward data transactions are executed autonomously by the onboard data handling subsystem without requiring ground intervention.

Off-nominal operational states are managed through a defined hierarchy of contingency responses — including onboard packet retention, scheduled retransmission upon link re-establishment, and dynamic ISL-assisted rerouting invoked autonomously whenever a primary delivery path is unavailable.

2. REQUIREMENTS ANALYSIS

The MediSat requirements baseline has been developed in accordance with ECSS-E-ST-10C [6] and ECSS-E-ST-10-06C [3], following a structured, traceable, and top-down systems engineering approach. The objective of this process is to ensure that all technical requirements are Traceable to mission objectives and user needs, Functionally justified through system-level analysis, Verifiable through defined verification methods (Test, Analysis, Inspection, Review) and Free from implementation bias, in accordance with ECSS principles. The requirements baseline serves as the authoritative reference for system design, verification, and subsystem allocation, ensuring consistency across all engineering deliverables.

2.1. Requirements Derivation Process

The MediSat requirements baseline is derived through a structured, top-down transformation process consistent with ECSS systems engineering practices. The way MediSats requirements have been defined can be seen on fig. 2. This process ensures traceability from mission objectives to verifiable subsystem requirements and maintains a clear separation between functional intent and implementation. The decision making process is illustrated in figure 2.

The derivation process consists of the following stages:

1. **Mission Objectives Definition:** High-level mission goals are established, such as secure and delay-tolerant medical data relay.
2. **User Needs Identification:** Operational expectations from stakeholders are captured, including reliability, autonomy, and data security.
3. **Functional Analysis:** The mission is decomposed into discrete system functions, including data acquisition, storage, routing, and transmission.
4. **Functional Architecture Development:** Functions are allocated across system elements and subsystems in accordance with the MediSat functional architecture defined in the DDF.
5. **System-Level Requirement Formulation (TRS):** Functions are translated into clear, measurable, and verifiable requirements using ECSS-compliant "shall" statements.
6. **Requirement Allocation and Decomposition:**
   - System requirements are allocated to subsystems where responsibility is unambiguous.
   - Requirements are refined into subsystem-level specifications (SS-TRS), ensuring strict traceability and avoidance of design leakage.
7. **Verification Definition:** Each requirement is assigned a verification method (Test, Analysis, Inspection, or Review of Design), ensuring compliance can be demonstrated within the Verification Plan framework.

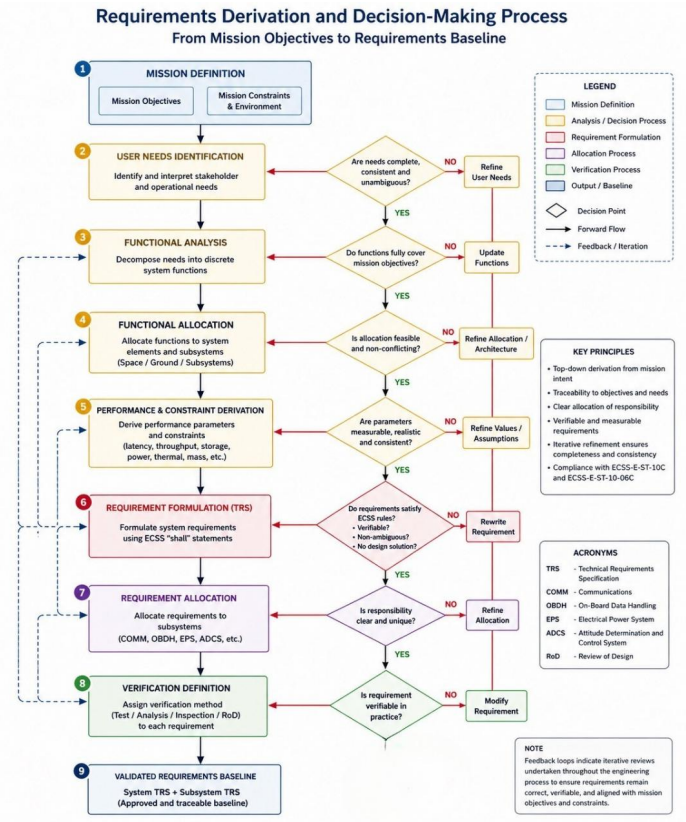

Figure 2. Requirements definition and decision making process

2.2. Mission Objectives and User-Centric Design

Core of the MediSat mission is defined by the operational requirements of medical personnel and humanitarian responders in the field. To ensure efficacy, the system prioritizes several high-level user needs:

- Reliable Data Transport: The architecture must guarantee the secure transport of medical records and diagnostics despite intermittent network coverage.
- Delay-Tolerant Connectivity: Utilizing a store-and-forward mechanism, the system ensures that data reaches its destination even when real-time end-to-end connectivity is unavailable.
- Operational Simplicity: Recognizing that field operators may not be satellite experts, ground terminals are designed for rapid deployment with intuitive, icon-based interfaces.

- Security and Compliance: The mission mandates rigorous data integrity and confidentiality through AES-256 and RSA-2048 encryption [2], [11], adhering to global healthcare standards such as HL7/FHIR [9] and privacy regulations like GDPR [8].

2.3. Functional Requirements and Data Handling

The MediSat system defines an end-to-end data handling chain based on delay-tolerant networking principles. The system shall be capable of:

- Encapsulating, storing, routing, and forwarding data across intermittently connected nodes
- Prioritizing data flows based on mission-defined urgency levels
- Maintaining minimum communication performance (e.g., throughput and availability)
- Autonomously scheduling communication sessions and managing network resources
- Ensuring operational continuity through Fault Detection, Isolation, and Recovery (FDIR)

These functional capabilities are translated into measurable system-level requirements and allocated to the relevant subsystems.

2.4. Space Segment Requirements

The space segment requirements define the constraints necessary to achieve the required coverage performance, access continuity, and operational reliability. The system shall provide:

- Sufficient access opportunities over mission-relevant regions
- Onboard storage capacity to support delay-tolerant operations
- Autonomous operation capability during communication outages
- Compliance with mission lifetime and environmental constraints
- Compatibility with CubeSat platform mass, volume, and deployer limits

These requirements drive constellation sizing, orbital design, and spacecraft platform definition.

2.5. Ground segment Requirements

The system architecture includes a ground segment responsible for mission operations, data handling, and user interfacing. Key requirements include:

- Portable and rapidly deployable user terminals
- Compatibility with distributed ground station infrastructure
- Secure data transfer and regulatory compliance
- Centralized mission operations and data management

These constraints ensure that the end-to-end system remains operationally effective in disaster-response scenarios.

2.6. Subsystem Allocation and Technical Constraints

The technical burden is distributed across specialized spacecraft subsystems, each governed by derived technical requirements:

- Communication (COMM): Responsible for bidirectional S-band and X-band links, as well as inter-satellite relay capabilities.
- On-Board Data Handling (OBDH): Manages command execution, data storage logic, and the validation of DTN bundle structural compliance
- Electrical Power System (EPS): Scaled to handle peak communication loads and ensure survivability during 39-minute eclipse periods.
- Attitude Determination and Control (ADCS): Ensures the pointing accuracy ($\leq 0.5°$) and stability ($\leq 0.05°$ RMS) required for high-bandwidth communication links.
- Thermal and Structural: The thermal subsystem maintains components within a $-10°C$ to $120°C$ range, while the structure provides the mechanical integrity needed to survive 10 g RMS launch vibrations.

3. SYSTEM DESIGN

Each design element for the MediSat mission is derived directly from the mission's operational concept: the requirement for resilient, secure medical data relay across the Pacific Ring of Fire. The system is decomposed into two principal segments — space and ground — whose interfaces are governed by open standards to ensure interoperability, scalability, and regulatory compliance. The following subsections detail the constellation architecture, network architecture and satellite platform specification.

3.1. Constellation Architecture

The MediSat space segment is designed as a reusable disaster-response communications infrastructure, demonstrated through a mission case focused on the Pacific Ring of Fire [14] (see fig. 3, below), selected as a representative high-risk region for constellation sizing and validation. The mission reference nodes—Manila, Tokyo, Jakarta, Santiago, and San Francisco—capture geographically distributed disaster-prone areas where resilient medical data relay may be required during terrestrial infrastructure outages.

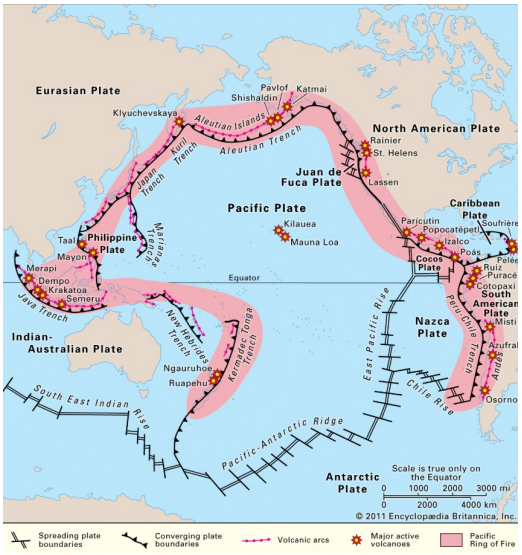

Figure 3. Map of Pacific Ring of fire showing regions prone to volcanic activity

The Support for disaster-resilient communications as a system driver is consistent with guidance from United Nations Office for Disaster Risk Reduction and World Health Organization. To support persistent regional service, MediSat adopts a Walker Delta 54/6/1 low Earth orbit constellation (see fig. 4) comprising 54 identical 12U CubeSats distributed over six orbital planes. The Walker architecture was selected for its balanced coverage geometry, regular revisit characteristics, distributed redundancy, and scalability, following established constellation design principles described in Space Mission Analysis and Design and the original Walker constellation methodology.

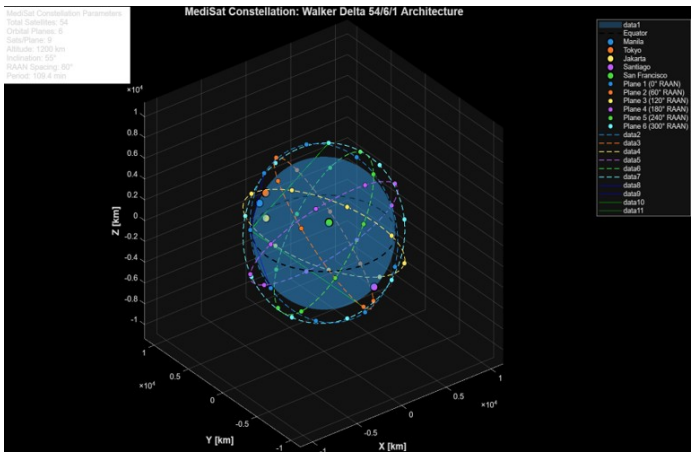

Figure 4. MediSat Walker Delta 54/6/1 three-dimensional orbital architecture

All spacecraft operate in circular 1200 km orbits at 55° inclination, with six orbital planes separated by 60° RAAN spacing and nine satellites per plane phased at 40° true anomaly increments. The Walker phasing parameter $f = 1$ introduces inter-plane offsets that stagger access opportunities and avoid temporal clustering of overpasses.

This geometry was selected specifically to maximize service continuity over the Pacific Ring of Fire latitude band while avoiding unnecessary polar over-coverage. Coverage simulations using SGP4 propagation with an elevation mask 10° indicate:

- > 99% single-satellite availability
- 82–94% dual-satellite visibility
- < 2 minute mean daily outage
- Continuous multi-pass access opportunities

At 1200 km altitude, each spacecraft provides an approximately 2670 km coverage footprint, representing a trade between coverage footprint, contact duration, latency, and constellation size, consistent with standard LEO constellation design practice [7].

3.2. Network Architecture

The MediSat constellation employs a hybrid distributed network architecture (see fig. 5) designed to support resilient medical data relay under intermittent connectivity and disaster-response operating conditions. The architecture combines mesh inter-satellite connectivity with star-like feeder routing toward ground-access nodes, balancing routing redundancy with efficient data delivery.

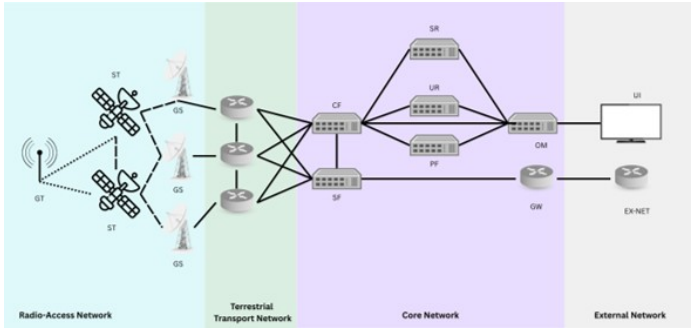

Figure 5. Medisat Logical Network Architecture

Within the space segment, satellites operate as distributed relay nodes connected through inter-satellite links (ISLs), enabling multi-hop forwarding when direct downlink opportunities are unavailable. In this store-carry-forward architecture, medical data may be routed across multiple spacecraft before reaching a ground station, improving service continuity during ground outages or unfavorable access geometry. Concept for the flow of data is seen on fig. 6.

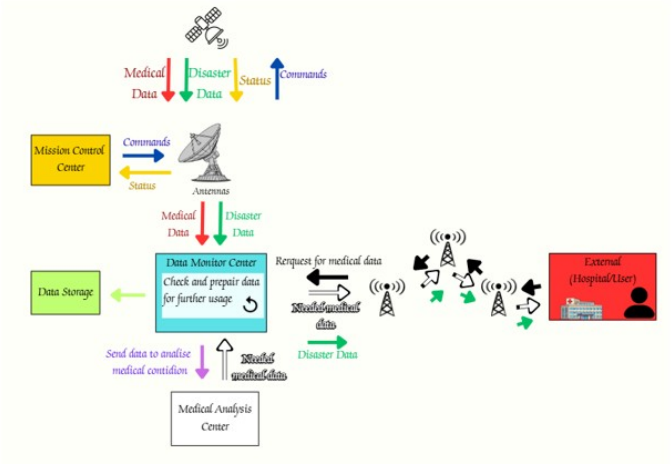

Figure 6. Data flow between satellites, terminals and ground stations

The mesh component provides multiple routing paths between nodes, increasing fault tolerance and allowing autonomous rerouting around unavailable satellites or congested links. Complementing this, star-like feeder routing directs traffic toward satellites with active ground contact, improving downlink efficiency and reducing routing complexity.

The networking layer is based on Delay/Disruption Tolerant Networking (DTN) principles, using custody-based forwarding and queued bundle transfer to tolerate intermittent links, scheduled contacts, and variable propagation delays. These routing concepts are aligned with Consultative Committee for Space Data Systems Bundle Protocol standards [10] and are well suited to distributed LEO relay systems. This hybrid architecture enables:

- resilient end-to-end medical data delivery.
- multi-path routing redundancy.
- tolerance to satellite and ground-node outages.
- scalable distributed constellation operations.

The approach follows architectural heritage established by Iridium Communications [1] and modern proliferated LEO relay networks such as SpaceX [12], while being adapted here for delay-tolerant humanitarian communications rather than broadband service.

3.3. System Architecture

The architecture of the MediSat system (illustrated in fig. 7) is organized into two primary segments: the space segment and the ground segment, interconnected through bidirectional communication links. The space segment consists of a distributed constellation of spacecraft interconnected via inter-satellite links (ISLs), forming a cooperative relay network that enables data transfer across the constellation. Each spacecraft can exchange data with neighboring nodes, allowing medical information to be routed dynamically through the network when direct ground contact is unavailable. The ground segment comprises mission control and user terminals, where mission control manages telemetry, tracking, and command (TT&C) operations, while user terminals serve as the interface for medical personnel to upload and receive data. Medical data flows from user terminals to the space segment, is relayed across the inter-satellite network, and is subsequently downlinked to ground infrastructure and forwarded to medical centers. This architecture supports delay-tolerant, multi-hop data delivery while maintaining centralized control through mission operations. The architecture was designed in such a way as to provide for the ability to exchange medical information reliably, securely, and without delays through conditions where connection is intermittent and ground communications infrastructure is unreliable. Based on the constellation concept introduced in Section 3.1, the architecture con-

sists of a distributed and autonomous network, where each satellite works as an intelligent node in the space communications network.

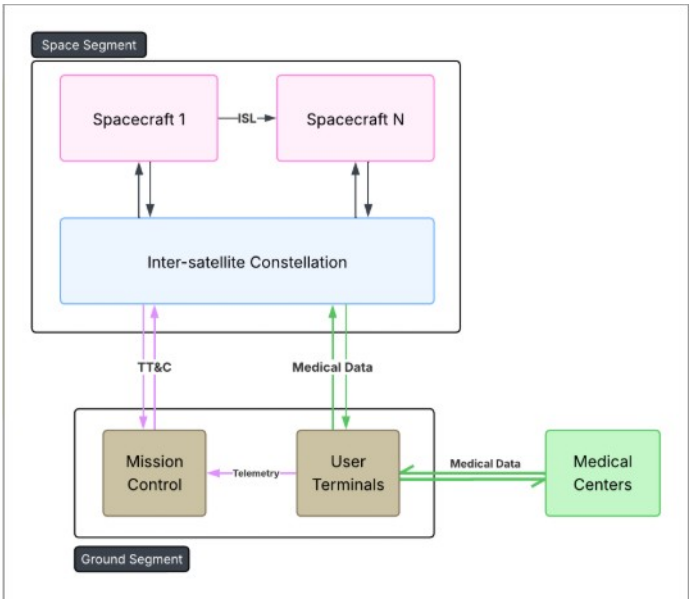

Figure 7. System Architecture

The fundamental aspect of the system architecture is the implementation of a store-and-forward communication network, based on the concepts of the Delay Tolerant Network (DTN). The medical data is packed into small data packets and processed asynchronously by the network. Each satellite can perform data reception, validation, storage, prioritization, and retransmission in accordance with current network topology and connectivity.

This architecture encompasses three major forms of communication networks: uplinking from users to satellites, inter-satellite communication links (ISLs), and downlinking from satellites to the ground. Through this multi-hop communication model, information can pass through the constellation network irrespective of the lack of immediate connectivity with the ground stations. The ISLs help to ensure continuity of communication by providing connectivity across different orbital planes in order to avoid coverage gaps as normally encountered in disaster-prone areas.

One of the major aspects of the design of this constellation network is autonomy. Due to the limited nature of interaction with the ground, it is necessary for the satellites to independently carry out communication planning and make decisions on information routes. This would also involve prioritising medical information as per the priority level assigned by the users in the ground terminals.

The architecture also incorporates end-to-end data security and integrity mechanisms. Data is encrypted at the source and remains protected throughout its transmission across the space and ground segments. The data transmission has to be compliant with numerous regulations around the globe like Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR).

The system architecture, therefore, translates the mission requirements for secure, delay-tolerant medical data relay into a cohesive technological framework, integrating networking, autonomy, and distributed space infrastructure to achieve resilient end-to-end communication.

3.3.1. Ground segment Architecture

The MediSat ground segment provides the interface between the space segment and end users, enabling mission operations, data relay, and user interaction under both nominal and degraded conditions. It comprises a distributed network of ground stations and portable user terminals (see fig.8), coordinated through a centralized Mission Operations Centre (MOC). The ground segment enables bidirectional communication with the satellite constellation for telemetry, tracking, and command (TT&C), as well as prioritized medical data downlink and distribution.

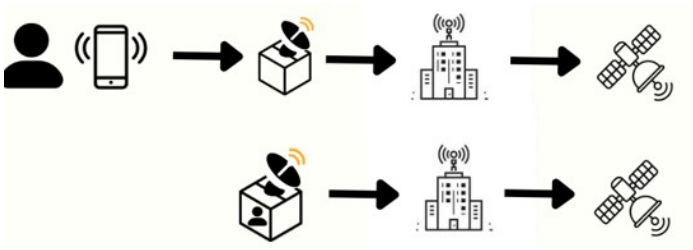

Figure 8. Ground segment operations

The ground station network adopts a distributed architecture, leveraging compatibility with scalable infrastructures such as SatNOGS [15] . This approach increases geographical diversity, enhances contact availability, and mitigates single-point failures. By enabling opportunistic access to any satellite in view, the system reduces latency and improves robustness, particularly in disaster scenarios where local infrastructure may be compromised.

The placement of ground stations and user terminals (see fig.9) is guided by the mission focus on the Pacific Ring of Fire [14], with nodes positioned to provide coverage over geographically distributed, disaster-prone regions including Southeast Asia, Japan, and the west coasts of North and South America. This localisation ensures that each target region has frequent access opportunities to at least one ground node, reducing latency and improving data delivery reliability. By aligning ground infrastructure with regions of high seismic and volcanic activity, the system ensures that data generated in affected areas can be downlinked with minimal delay, even in scenarios where terrestrial communication systems are disrupted.

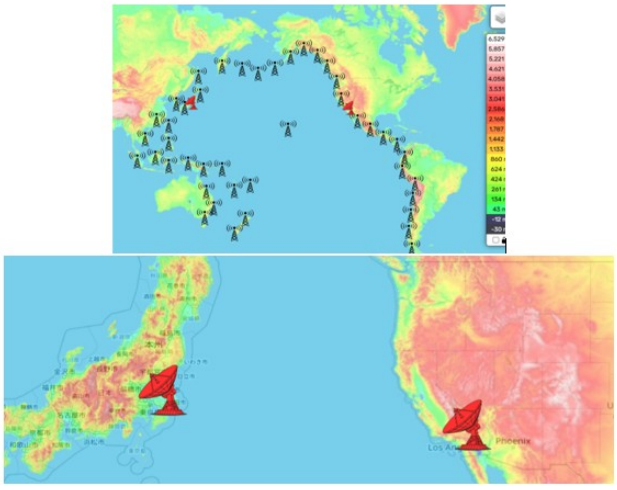

Figure 9. Ground segment operations

User terminals serve as the primary interface for field medical personnel and are designed for rapid deployment in austere environments. Each terminal supports local data acquisition, temporary storage, and uplink to the satellite network using delay-tolerant networking principles. A minimum operational endurance of 8 hours on battery power ensures functionality in power-constrained scenarios, while simplified interfaces enable operation by non-specialist users.

3.3.2. Ground segment Performance and Access Characteristics

The performance of the ground segment is directly driven by the constellation geometry and resulting access characteristics. Frequent satellite passes enable multiple daily contact opportunities, with typical contact durations of 5–12 minutes per pass. Combined with a minimum downlink capability of 10 Mbps, this allows significant data volumes to be transferred within each visibility window.

The distributed ground station network further increases effective access opportunities, enabling data to be downlinked through any available station. In conjunction with delay-tolerant networking based on Consultative Committee for Space Data Systems Bundle Protocol standards [10], data may be stored onboard satellites and forwarded across the constellation until a suitable ground contact is established. This ensures reliable data delivery even under intermittent connectivity conditions.

From a system perspective, the integration of constellation design, distributed ground infrastructure, and DTN-based routing enables a robust end-to-end data delivery chain. This architecture satisfies system-level requirements for availability, latency, and throughput, even in disaster-response scenarios where terrestrial communication networks may be degraded or unavailable. A summary of performance specifications are detailed in table 1

Table 1. Ground Segment and User Terminal Performance Summary

Parameter	Value / Capability
Downlink data rate	$\geq$ 10 Mbps
Contact duration	5–12 minutes per pass
End-to-end latency	Minutes (DTN store-and-forward)
Access strategy	Opportunistic multi-satellite access
Ground network	Distributed, SatNOGS-compatible
User terminal power	$\geq$ 8-hour battery operation
Deployment	Portable, rapid deployment
Data handling	Local storage + DTN-compatible upload
Interface	Low-complexity, non-expert operation
MOC capability	Centralized scheduling and routing
Security	Encrypted data transfer and compliance

4. SUBSYSTEM DESIGN

The MediSat system architecture is realized through a set of tightly integrated spacecraft subsystems, each responsible for a distinct set of functions derived from system-level requirements. Following the ECSS-aligned systems engineering approach, subsystem design is driven by requirement allocation, ensuring that performance, resource, and operational constraints are satisfied at both component and system levels. The spacecraft is decomposed into the primary subsystems— COMM, OBDH, EPS, ADCS, Thermal, and Structural—each contributing to the overall functionality and reliability of the mission. Design decisions at subsystem level are guided by mass, power, thermal, and operational budgets, as well as the need for robustness under launch and on-orbit environments. The following sections present the design and justification of each subsystem, emphasizing their role in achieving end-to-end system performance for resilient medical data relay.

4.1. Communication Subsystem

The Communications subsystem, is responsible for controlling and executing data transfers for both payload and TT&C streams between Medisat's ground segment, including ground terminals, and the space segment, while also interfacing with external networks. More specifically, it manages data transfer scheduling, resource allocation, link establishment and control, channel estimation, and mobility. COMM operates primarily at the physical and data link layers, and to a limited extent at the network layer. Higher-layer functions associated with data transfer are handled by OBDH and ground segment data processing. The COMM subsystem is designed in accordance with ECSS-E-ST-50C standards [4] among others.

The subsystem architecture is divided into the physical and link layers. The physical layer manages bit-level encoding, modulation, and transmission across the medium, while the link layer ensures data integrity through frame-level reassembly checks and error correction.

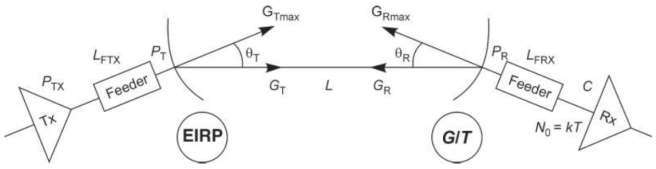

Figure 10. Typical front end

The communication front-end (see fig. 10) serves as the interface between digital processing and electromagnetic propagation. To optimize signal quality, the design incorporates specific component chains for both transmission and reception:

- Transmitter Chain: Consists of filters, modulators, a High Power Amplifier (HPA), and the antenna assembly.
- Receiver Chain: Utilizes filters, modulators, and a Low Noise Amplifier (LNA) to maximize the Signal-to-Noise Ratio (SNR) of incoming data.

To support a multi-tiered communication architecture, Medisat utilizes X, L, and K bands across different operational planes. The system distinguishes between user-facing data links and telemetry, tracking, and command (TT&C) functions. Below on table 2 is a summary of communication link parameters.

Link Case	Band	Bandwidth	Throughput	Antenna Type	EIRP
Uplink (Portable)	X Band (10 GHz)	15 MHz	15 Mbps	4x4 Patch Array	25–30 dBW
Uplink (Stationary)	X Band (10 GHz)	15 MHz	20 Mbps	Parabolic	47 dBW
Downlink (Data)	X Band (8 GHz)	15 MHz	20 Mbps	Patch/Horn	27–32 dBW
Intersatellite	K Band (22 GHz)	10 MHz	40 Mbps	64x64 Patch Array	43 dBW

Table 2. Communication link parameters

4.2. OBDH subsystem

The OBDH subsystem serves as the CubeSat's central digital hub, responsible for onboard command and control, secure store-and-forward management of mission and payload data (e.g., medical records), system health monitoring, and data routing between internal subsystems and external communication links (ground and inter-satellite). The hardware-software solution is based on a dual-processor Raspberry Pi Compute Module architecture, and incorporates eMMC mass storage, a hardware watchdog, a battery-backed real-time clock (RTC), redundant internal communication buses (I^2C and SPI), and interfaces to the EPS, ADCS, Thermal, and Communications subsystems, the data exchange between these subsystems is shown in fig. 11.

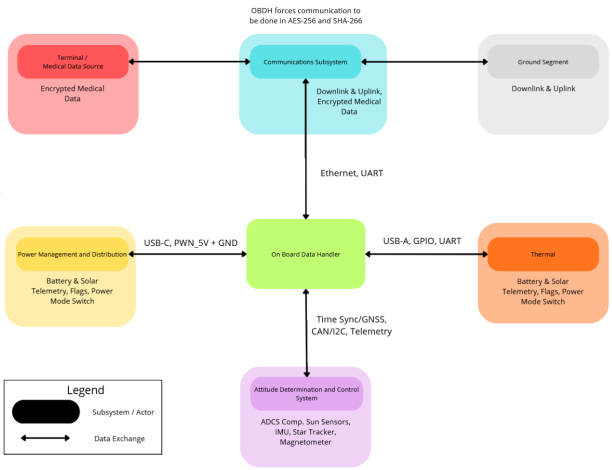

Figure 11. Block diagram of OBDH's key interfaces

To endure the harsh conditions of low Earth orbit, the OBDH architecture centers on a dual-processor design utilizing two Raspberry Pi Compute Module 5 (CM5) units.

- Each CM5 features a 1.5GHz quad-core ARM Cortex-A72 processor and 6GB of DDR4 RAM.
- The primary non-volatile storage is a 32GB space-grade eMMC flash module (UT8MNQ32GBeMMC51), selected for its relative resilience against Total Ionizing Dose (TID) effects.
- Hardware-level protections include ECC-protected memory for critical buffers, a hardware watchdog timer capable of triggering system resets during deadlocks, and a battery-backed real-time clock (RTC) for accurate temporal tracking across power cycles.

The software framework utilizes a hierarchical approach balancing real-time execution with mission flexibility. The framework has been defined in accordance to the guidelines in ECSS-E-ST-40C standard [16]. The operating system is built on a minimal Linux distribution tailored for embedded space applications, featuring a read-only root partition to prevent file system corruption alongside separate writable partitions for mission data.

- Real-Time Core (C++): Critical, performance-sensitive functions—such as the Core Command & Control, Data Buffering Engine, and the Error Correction Module (employing Reed-Solomon coding and CRC checks)—are developed in C++ to ensure optimal hardware interaction.
- Orchestration Layer (Python): Higher-level operations, including the Communication Scheduler and Health Monitoring Daemon, are implemented in Python for adaptability.

To handle network congestion or anomaly events, the system implements an Emergency Protocol Handler. This module is responsible for dynamically reprioritizing queued messages to guarantee the delivery of life-critical data. This dynamic Quality-of-Service mechanism ensures that time-sensitive information is immediately moved to the front of the transmission queue, prioritizing it over routine telemetry or lower-urgency data. Furthermore, an AI Filter Interface is integrated to pre-process, rank, and validate incoming medical data uplinked to the satellite. By ranking this data by urgency - as seen on fig. 12 - the system minimizes bandwidth consumption and ensures that only relevant, high-priority information is processed and transmitted. The key software modules can be found in table 3.

Module	Functionality	Language or Tech Stack
Core Command & Control	Real-time task execution, scheduling, system state management	C++
Data Buffering Engine	Store-and-forward queue for payload and telemetry data	C++, SQLite
Security Layer	AES-256 encryption, RSA-2048 key exchange, SHA-256 hashing	C++, crypto API
File System Handler	Read-only OS partition, writable log/data partitions	Linux (ext4), OverlayFS
Communication Scheduler	UHF/VHF/S-band scheduling and modulation control	Python, C++, shell scripting
Error Correction Module	Reed-Solomon & CRC encoding/decoding for transmission integrity	C++
Health Monitoring Daemon	Monitors CPU temp, voltage, uptime; triggers watchdog resets	Python
Emergency Protocol Handler	Reprioritizes traffic during anomaly or congestion events	Python
AI Filter Interface	F Ranks incoming uplink data by urgency to optimize bandwidth	Python, TensorFlow Lite
Logging & Diagnostics	Persistent log handling and diagnostic event reporting	Python, rsyslog/journald
Update Manager	Handles OTA updates for non-critical modules and payload interface logic	Bash, Python, systemd timers

Table 3. Key Software Modules for OBDH

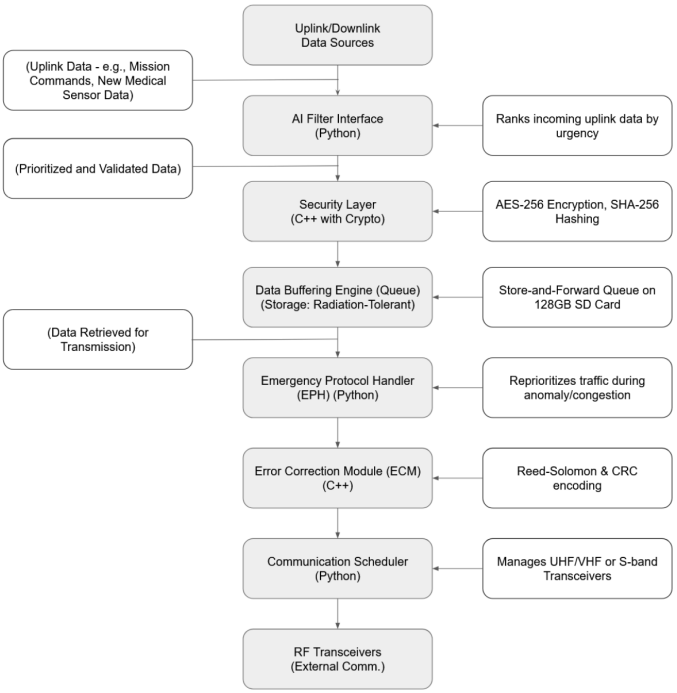

Figure 12. Software prioritisation logic

4.3. ADCS subsystem

The ADCS provides three-axis attitude determination and closed-loop control across all mission phases, supporting antenna pointing for ground and inter-satellite links (ISL), solar array sun-tracking for power generation, and thermal stability through controlled spacecraft orientation. Operating within an autonomous store-and-forward constellation, each satellite must function as a stable, self-sufficient communication node, placing stringent demands on pointing perfor-

mance. The subsystem is designed to achieve a combined pointing accuracy of 0.23° (3 sigma)(eqn 1), derived from a root-sum-square (RSS) error budget across three contributor categories: alignment residuals, attitude knowledge errors, and control accuracy.

$$\sigma_{\text{ADCS}} = \sqrt{\sigma^2_{\text{align}} + \sigma^2_{\text{knowledge}} + \sigma^2_{\text{control}}} \quad (1)$$

Key contributors include star tracker mounting residuals (0.03°), gyro bias residuals (0.05°), estimator tuning residuals (0.03°), and controller steady-state error (0.06°). This satisfies system-level requirements of ±0.5° for ISL and ground link acquisition, and 0.05° RMS attitude stability during communication bursts.

Attitude determination is achieved through multi-sensor fusion.

- The STAR TRACKER-ST200 serves as the primary fine attitude sensor in nominal operation, delivering quaternion-based solutions compatible with pointing requirements.
- Angular rate sensing is provided by the IADCS-100 embedded IMU, which remains active across all modes including detumble and safe mode.
- Coarse Sun vector knowledge is provided by FSSA-110 sun sensors, supporting sun-pointing during safe mode and degraded scenarios.
- The MAG-3 three-axis magnetometer provides geomagnetic field measurements for coarse attitude aiding and magnetorquer feedback during detumbling and momentum dumping.

Attitude control is result of actuator control which has the following components:

- Fine three-axis control is achieved using four RW1 Type A reaction wheels arranged in a pyramid configuration, providing redundancy under single-wheel failure.
- Magnetorquers (VIBES-MACS, ×3, orthogonally mounted) serve as primary actuators during initial detumbling and perform scheduled reaction wheel desaturation by interacting with the Earth's magnetic field.

This hybrid architecture (see fig. 13 below) ensures of robustness against disturbances including atmospheric drag, solar radiation pressure, and residual magnetic torques.

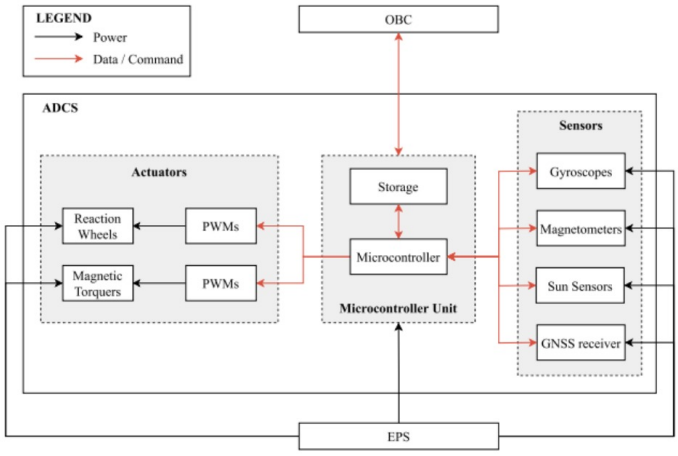

Figure 13. Block diagram of ADCS subsystem

For control architecture the subsystem runs on a closed feedback loop. A quaternion-based estimator fuses sensor measurements in real time, with star tracker data providing the primary attitude reference and gyro measurements propagating attitude between updates. In the absence of valid star tracker data, the estimator transitions to a degraded mode using IMU propagation aided by sun sensor and magnetometer measurements. Mode-dependent control laws govern actuator output:

- Reaction-wheel-based control is used in nominal, ISL, and ground communication modes.
- Magnetorquer-based control dominates during detumble and safe mode to minimize power draw

Momentum accumulation is continuously monitored and managed through scheduled desaturation, coordinated to avoid interference with communication windows.

4.4. EPS subsystem

The EPS is designed to provide constant electrical energy supply to all the systems onboard during any phase of the mission. Considering that transmitting large amounts of data requires significant power, the EPS will have the capability to balance out power requirements throughout full orbits, including eclipses of up to 39 minutes in duration, without additional control from ground operators.

Electrical energy is produced using deployable solar panels consisting of four 2×3U panels and one 2×2U stationary panel, like shown on fig. 14, thereby utilizing maximum available surface area in a 12U CubeSat. Voltage and current from each solar panel are controlled by a Maximum Power Point Tracking (MPPT) device. With the sun tracking ability provided by the ADCS, the system can produce around 101.27 Wh in each orbit; however, towards the end of the mission life, due to solar panels degradation, this will be reduced to 96.20 Wh per orbit.

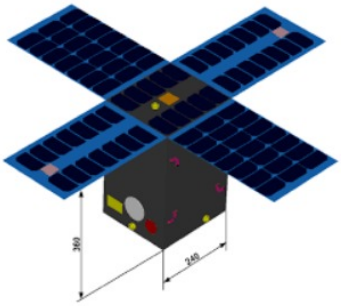

Figure 14. Solar array setup

A 100 Wh lithium-ion rechargeable battery provides energy storage for eclipse operations and pre-launch and launch phases. To limit capacity degradation from charge/discharge cycling, the nominal depth of discharge (DoD) is capped at 40% per cycle, preserving battery lifetime across the mission. The battery is sized to sustain satellite operations through at least one full eclipse cycle at both beginning and end of life.

Power distribution is managed through a centralised Power Management and Distribution (PMAD) system, incorporating load balancers and DC-DC converters to deliver regulated voltage across 14 individually switched subsystem ports. The PMAD operates at a solar bus voltage of approximately 40 V, stepping down to 5 V regulated outputs for subsystems including the OBDH. Core functions of the PMAD include power management, load balancing, continuous voltage monitoring, and fault isolation. Critical subsystems are connected via dual redundant paths routed separately through the spacecraft to ensure continued operation under wiring faults. A conceptual diagram is visible on fig. 15, below.

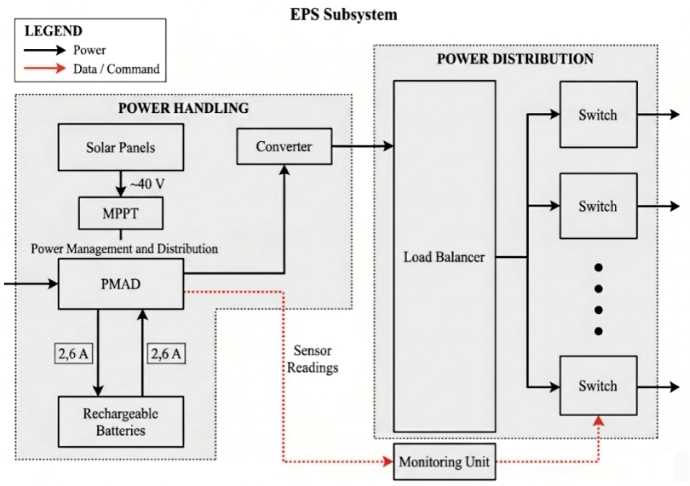

Figure 15. Block diagram for EPS subsystem

Total power consumption varies across mission phases where key values include 0.2 W during pre-launch and launch modes (L1–L2), rising to 37.8 W during separation (L3) and 32.4 W during nominal data relay operations (S2). With an orbit period of 109 minutes, 70 minutes of sunlight are available for recharging, against a total orbital energy consumption of 72.69 Wh — comfortably within the 101.27 Wh generation capacity.

4.5. Thermal subsystem

The thermal subsystem is designed to maintain all spacecraft components within their operational and survival temperature limits under worst-case orbital conditions, while minimizing power consumption and system complexity. A passive-dominant thermal control architecture is adopted, combining multi-layer insulation (MLI), radiator-coated external panels, conductive thermal paths, and localized survival heaters.

Thermal analysis (table 4) indicates that all subsystems remain within allowable temperature limits with 10°C margin across both hot and cold cases. Communications hardware operates within a nominal range of approximately +2°C to +30°C, remaining well inside its operational limits, while structural elements and internal avionics remain within safe bounds throughout eclipse and sunlight transitions. No active cooling is required, and heater usage is limited to cold-case survival modes, reducing power demand and improving overall system efficiency. This demonstrates compliance with ECSS thermal control practices [5] and validates the passive thermal design approach.

Table 4. Thermal Subsystem Temperature Budget

Subsystem	Predicted Range [°C]	Operational Limits [°C]
Communications	2 to 30	0 to 40
OBDH	5 to 35	0 to 50
ADCS	-5 to 25	-10 to 50
Structure	-20 to 5	-55 to 100
Battery	10 to 25	0 to 40

The thermal architecture (see fig. 16) is closely coupled with subsystem placement and structural interfaces. High-dissipation components, particularly within the communications subsystem, are mounted on panels with direct conductive paths to radiator surfaces to enable efficient heat rejection. Conversely, temperature-sensitive components such as batteries and avionics are thermally isolated and positioned away from external radiators to reduce exposure to cold-case conditions. Conductive coupling through the structural frame is used to distribute heat loads, while MLI minimizes radiative exchange with the space environment.

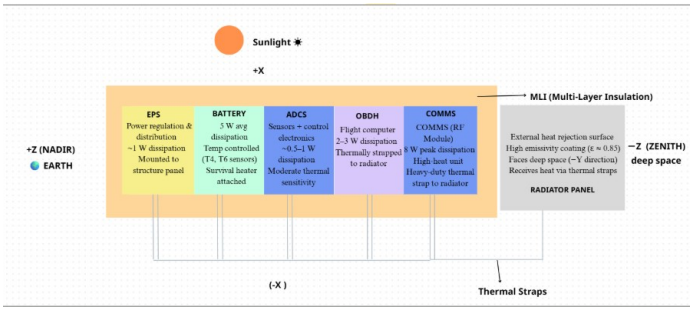

Figure 16. Thermal management architecture

Heater placement is localized to critical components to ensure survival during eclipse without introducing unnecessary system-level power penalties. This placement strategy ensures that thermal gradients are controlled, hot spots are mitigated, and subsystem temperature limits are maintained under all mission phases. The resulting design reflects a system-level thermal philosophy where component placement, structural conduction, and radiator utilization are co-optimized, consistent with established small satellite thermal design practices and European Cooperation for Space Standardization thermal control [5] guidelines.

4.6. Structural subsystem

The structural subsystem design is driven by the system-level mass budget and packaging requirements of the MediSat 12U platform. The spacecraft dry mass is estimated at 17.71 kg, with the communications subsystem (including payload and inter-satellite link hardware) representing the dominant mass contributor. The estimated mass budget is outlined in table 5. This mass distribution directly informs the selection of the primary structural architecture, as the frame must support a communications-heavy payload while maintaining stiffness, alignment stability, and deployer compatibility.

Table 5. MediSat System Mass Budget

Subsystem	Mass [kg]
Communications (incl. payload & ISL)	8.05
Structure	3.90
EPS	3.21
ADCS	1.30
Thermal	0.74
OBDH	0.51
Total Dry Mass	**17.71**

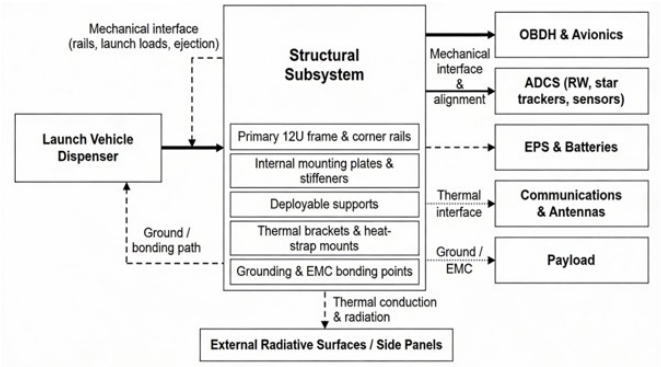

Figure 17. Functional block diagram of structural subsystem

To meet these requirements, a flight-heritage NPC Spacemind SM12 12U structure was selected. The structural subsystem carries an allocated mass of approximately 3.9 kg, including the primary frame, internal mounting plates, deployable supports, and interface hardware, with a 20% structural mass margin maintained at PDR. The

selection prioritizes structural robustness and integration reliability over aggressive mass minimization, ensuring compatibility with subsystem accommodation and late-stage integration growth. A fig. 17 above shows diagram describing the structural system.

The structure is qualified to withstand 10–15 g quasi-static launch loads, random vibration, and shock environments typical of CubeSat deployments, while preserving subsystem alignment and thermo-elastic stability required for high-precision communications and ADCS performance. This approach is consistent with established small satellite structural design practices described in Space Mission Analysis [7] and Design and the CubeSat Design Specification [13], where structural architecture is driven by system mass closure, launch environment compliance, and integration constraints.

5. VERIFICATION AND VALIDATION METHODS

5.1. Verification Approach

The MediSat verification strategy is compliant with the ECSS-E-ST-10-02C standard and thus provides the framework against which all planning, implementation, and evidence closure actions will be performed throughout the project cycle. Each system technical requirements specification is allocated one or more among the four allowed techniques

- Inspection: Visual and documentary examination of physical properties and workmanship.
- Analysis: Theoretical evaluation, including performance modeling, thermal calculations, and link budget analysis.
- Review of Design: Formal examination of approved design documentation and interface control documents.
- Test: Operating hardware and software under controlled conditions, encompassing functional, environmental, and end-to-end testing.

5.2. Model Philosophy

Balancing development efficiency with risk containment—a crucial trade-off in academic systems engineering—the MediSat mission adopts a Proto-Flight Model (PFM) verification philosophy. Instead of manufacturing a complete, separate qualification model, a single flight-representative spacecraft is built and subjected to a combined qualification and acceptance test campaign.

To mitigate risks early in the development lifecycle, the project relies on a hierarchical model set:

- Engineering Models (EMs): Used for structural, electrical, and data-handling verification to confirm mechanical compatibility and functional behavior before final integration.
- FlatSat Configuration: An accessible testbed enabling system-level functional testing, software verification, and DTN data-flow validation.
- Proto-Flight Model: The final flight unit that undergoes full environmental and functional testing prior to launch.

Verification is structured across three hierarchical levels — Mission, System, and Subsystem — and four sequential stages: Qualification (Q), Acceptance (A), Pre-Launch (PL), and In-Orbit (IO). Subsystem-level compliance is established independently before integration, with system-level AIT following a defined bottom-up sequence. Formal review milestones including TRR and FAR govern phase progression and evidence closure.

5.3. Subsystem Integration and Testing Strategy

The Assembly, Integration, and Test (AIT) workflow follows a structured sequence designed to establish a stable physical and electrical baseline before introducing functional complexity. The integration sequence is illustrated by a diagram on fig. 18 and proceeds as follows:

- Structure and Mechanisms: Validation of primary load paths, stiffness, and deployer compatibility.
- EPS: Verification of power generation, energy storage, regulation, and distribution capabilities.
- OBDH: Testing of the dual-processor architecture, secure storage of medical data, and validation of DTN bundle routing.
- Communications: Verification of X-band, L-band, and optical inter-satellite links, alongside CCSDS protocol compliance.
- ADCS: Closed-loop testing of sensor data acquisition, actuator commanding, and fault detection.
- Thermal Control: Final integration utilizing stable electrical configurations to verify survival temperatures, heater functionality, and thermal gradients.

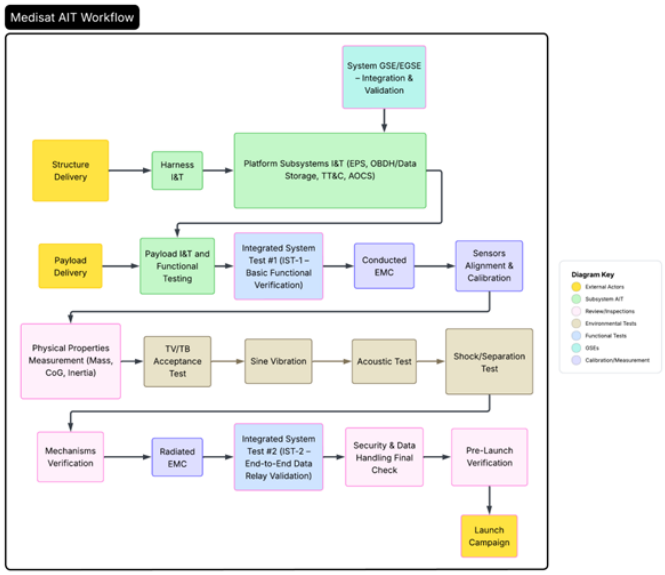

Figure 18. AIT workflow

5.4. System and Constellation-Level Verification

System-level verification spans both the space segment (the 12U CubeSat platform and payloads) and the ground segment. Early functional correctness is validated using an Avionics Test Bench (ATB), allowing software and data handling concepts to be verified prior to hardware manufacturing.

The PFM undergoes an extensive environmental test campaign to verify survival and operational integrity. This campaign includes:

- Integrated System Tests (IST-1 and IST-2): Establishing functional baselines before and after environmental exposure.
- Environmental Testing: Including conducted and radiated Electromagnetic Compatibility (EMC), Thermal Vacuum (TVAC) testing, sine vibration, acoustic testing, and shock/separation tests.

At the constellation level, testing physical hardware on the ground is largely impractical; therefore, verification relies heavily on emulation and analysis. End-to-end multi-satellite data relay tests are conducted to validate DTN routing, data storage, and latency across multiple satellite hops. Final constellation verification is achieved during the In-Orbit Verification (IOV) phase, which confirms real-world geographic coverage, service availability, and space-ground interactions.

5.5. Verification Control

To maintain traceability across all verification stages, MediSat employs a strict Verification Control Methodology centralized around a Verification Control Document (VCD). The VCD maps every technical

requirement to its designated verification method, level, and the eventual objective evidence (such as test reports or analysis documents). Requirements are progressively closed through formal milestones, including the Preliminary Design Review (PDR), Critical Design Review (CDR), and Test Readiness Review (TRR), culminating in the Flight Acceptance Review (FAR)

6. CONCLUSION

The MediSat mission demonstrates a technically viable and systemically robust approach to enabling secure, delay-tolerant medical data relay in environments where terrestrial communication infrastructure is unavailable, degraded, or unreliable. By integrating a Walker Delta 54/6/1 LEO constellation with a distributed ground segment and DTN-based networking architecture, the system achieves high availability, low outage durations, and resilient end-to-end data delivery across geographically dispersed, disaster-prone regions, with particular focus on the Pacific Ring of Fire.

A key contribution of this work lies in the consistent application of an ECSS-aligned systems engineering methodology, ensuring traceability from mission objectives through functional decomposition to subsystem implementation and verification. The resulting architecture combines autonomous onboard data handling, prioritized store-and-forward communication, and secure data transmission mechanisms to meet the stringent requirements of medical data integrity, availability, and confidentiality. Subsystem designs have been shown to remain within CubeSat constraints for mass, power, and thermal performance, supporting the feasibility of the concept within a 12U platform.

The integration of distributed networking principles, inter-satellite links, and opportunistic ground access enables the system to maintain operational continuity under intermittent connectivity and partial system failures, achieving graceful degradation rather than service interruption. This highlights the suitability of the architecture not only for medical data relay, but also for broader disaster-response and humanitarian communication applications. Future work will focus on hardware prototyping, in-orbit validation of DTN routing performance, and scaling the architecture toward larger constellations and multi-mission integration. Additionally, further refinement of the onboard autonomy and intelligent data prioritization mechanisms could enhance the responsiveness of the system under extreme operational constraints. In general, MediSat illustrates how SmallSat constellations, when designed through a rigorous systems engineering framework, can extend beyond traditional applications to provide a resilient, secure, and scalable communication infrastructure for critical social needs.

7. BIBLIOGRAPHY

The references presented in this section provide the technical and regulatory foundation for the MediSat system design. They include established standards, academic literature, and industry sources that support the architectural choices, subsystem design, and networking approach adopted in this work. Together, these sources ensure traceability, validate key assumptions, and align the system with recognized engineering practices. An accompanying list of abbreviations is provided to ensure clarity and consistency in terminology throughout the paper.

ABBREVIATIONS

ADCS	Attitude Determination and Control System
AES	Advanced Encryption Standard
AIT	Assembly, Integration, and Test
CCSDS	Consultative Committee for Space Data Systems
COMM	Communication Subsystem
CRC	Cyclic Redundancy Check
DC-DC	Direct Current to Direct Current
DTN	Delay/Disruption Tolerant Networking
DoD	Depth of Discharge
ECC	Error Correction Code
ECSS	European Cooperation for Space Standardization
EM	Engineering Model
EMC	Electromagnetic Compatibility
EPS	Electrical Power System
FDIR	Fault Detection, Isolation, and Recovery
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
HPA	High Power Amplifier
IMU	Inertial Measurement Unit
ISL	Inter-Satellite Link
IST	Integrated System Test
LEO	Low Earth Orbit
LEOP	Launch and Early Orbit Phase
LNA	Low Noise Amplifier
MLI	Multi-Layer Insulation
MOC	Mission Operations Centre
MPPT	Maximum Power Point Tracking
OBDH	On-Board Data Handling
PFM	Proto-Flight Model
PMAD	Power Management and Distribution
QoS	Quality of Service
RAAN	Right Ascension of the Ascending Node
RMS	Root Mean Square
RTC	Real-Time Clock
SGP4	Simplified General Perturbations Model 4
SNR	Signal-to-Noise Ratio
TRR	Test Readiness Review
TRS	Teechnical Requirements Specifications
TVAC	Thermal Vacuum
TT&C	Telemetry, Tracking, and Command
V&V	Verification and Validation
VCD	Verification Control Document
EIRP	Effective Isotropic Radiated Power

REFERENCES

[1] B. Evans, “The Iridium Satellite System Architecture”, *IEEE Communications Magazine*, vol. 36, no. 3, pp. 44–51, 1998.

[2] NIST, *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001.

[3] European Cooperation for Space Standardization (ECSS), *Space Engineering – Technical Requirements Specification*, ECSS-E-ST-10-06C Rev.1, Noordwijk, The Netherlands, 2004.

[4] European Cooperation for Space Standardization (ECSS), *Space Engineering – Communications*, ECSS-E-ST-50C Rev.1, Noordwijk, The Netherlands, 2008.

[5] European Cooperation for Space Standardization (ECSS), *Space Engineering – Thermal Control General Requirements*, ECSS-E-ST-31C Rev.1, Noordwijk, The Netherlands, 2008.

[6] European Cooperation for Space Standardization (ECSS), *Space Engineering – System Engineering General Requirements*, ECSS-E-ST-10C Rev.1, Noordwijk, The Netherlands, 2009.

[7] J. R. Wertz, D. F. Everett, and J. J. Puschell, Eds., *Space Mission Analysis and Design*, 5th. Hawthorne, CA, USA: Microcosm Press, 2011.

[8] European Union, *General Data Protection Regulation (EU) 2016/679*, 2016.

[9] Health Level Seven International, *FHIR Release 4 (R4)*, 2019.

[10] Consultative Committee for Space Data Systems, *Bundle Protocol Specification*, CCSDS 734.3-B-1, Washington, DC, 2020.

[11] NIST, *Recommendation for Key Management*, NIST SP 800-57, 2020.

[12] M. Handley, "Using Ground Relays for Low-Latency Wide-Area Routing in Megaconstellations", *ACM SIGCOMM Computer Communication Review*, 2021.

[13] The CubeSat Program, California Polytechnic State University, *CubeSat Design Specification*, Rev. 14.1, San Luis Obispo, CA, USA, 2022.

[14] U.S. Geological Survey, *The Ring of Fire*, https://www.usgs.gov, 2023.

[15] Libre Space Foundation, *SatNOGS: Open Source Satellite Ground Station Network*, https://satnogs.org, 2024.

[16] European Cooperation for Space Standardization (ECSS), *Software Engineering Standards*, ECSS-E-ST-40C Rev.1, 2025. [Online]. Available: https://ecss.nl/standard/ecss-e-st-40c-rev-1-software-30-april-2025/.