QUARANET: EXECUTIVE ARCHITECTURE OVERVIEW

Next-Generation On-Board Cyber Resilience for Decentralized Space Networks

Abstract: Modern orbital networks and satellite constellations represent a paradigm shift in global communications, earth observation, and tactical data routing. However, as these assets scale, they face unprecedented exposure to localized cyber vectors, including signal manipulation, protocol disruption, and zero-day exploitation. Traditional defense methodologies relying on ground-based security layers are inherently decoupled from real-time orbital threats. Conversely, migrating terrestrial security applications directly to space is severely restricted by tight operational envelopes and harsh cosmic environments. This document presents the executive framework of QUARANET, a hardware-agnostic, zero-dynamic-allocation on-board cybersecurity framework. Engineered to operate directly within flight software layers, QUARANET replaces intensive processing pipelines with an elegant high-dimensional vector modeling architecture, delivering deterministic protection and structural fault tolerance without compromising critical mission resource parameters.

1. Context and Threat Evolution in New Space

The rapid expansion of the commercial and defense space sectors has led to the deployment of large-scale, interconnected satellite networks. These constellations act as critical, edge-computing infrastructure in orbit. Because these systems are highly interconnected, compromising a single node poses a systemic threat to the entire network topology.

Historical assumptions treated the space asset as an isolated entity protected entirely by the secure perimeter of its ground stations. Today, modern threat vectors target the space segment directly. Disruptive uplink transmissions, malicious cross-talk across inter-satellite links, and complex protocol attacks bypass perimeter defenses. Once a hostile packet reaches a flight computer, legacy systems often lack the decentralized intelligence required to recognize, isolate, and mitigate the threat natively at the asset level.

2. Constraints of Spaceborne Environments

Standard cybersecurity software cannot be deployed into space environments due to strict physical and operational limitations:

- **Thermal Management:** Space computers lack convection-based air cooling. Software that creates computational processing spikes induces localized heat buildup, risking electronic degradation or component failure.

- **Memory Volatility:** Terrestrial firewalls rely heavily on dynamic, on-demand memory structures to inspect traffic. Under high-volume network saturation, these structures risk exhausting available runtime memory, leading to critical system lockups or unplanned reboots.
- **Radiation Induced Anomalies:** Ionizing cosmic rays cause random bit alterations within semiconductor memory. Traditional algorithmic software relying on high-precision floating-point structures experiences severe execution errors or complete logic collapse when subjected to these environmental disruptions.

3. Core Innovation: High-Dimensional Invariance

QUARANET sidesteps the resource bottlenecks of conventional security applications by using a streamlined, high-dimensional vector space paradigm based on Hyperdimensional Computing principles. Rather than running exhaustive sequential inspections or compute-heavy matrices, incoming data is mapped into broad, distributed geometric profiles.

Security evaluation is performed via low-overhead geometric alignment checks. This allows the system to achieve highly predictable, deterministic execution intervals. Processing performance remains uniform and stable regardless of network traffic changes, ensuring that anomalous data streams cannot exhaust the host computer's resources.

Furthermore, because data patterns are represented globally across an extensive array of bits rather than concentrated in vulnerable pointers, the architecture exhibits high structural error tolerance. Minor memory changes caused by environmental radiation do not compromise the overall security assessment, providing built-in software resilience without requiring heavy physical shielding.

4. Implementation and Deployment Framework

The QUARANET framework is developed as a lightweight, bare-metal deployment module utilizing a highly structured, memory-safe language pipeline. It runs independently of any specific real-time operating system (RTOS) and sits cleanly within existing flight executive software stacks.

To guarantee operational predictability, the framework uses static memory structures and strict zero-copy processing. Incoming data packets are evaluated seamlessly through safe references without undergoing unnecessary duplication cycles. Thread management across processing units relies entirely on lock-free synchronization barriers, eliminating the risk of internal thread deadlocks or performance degradation during intense computational workloads.

5. High-Level Architectural Comparison

The matrix below contrasts the operational characteristics of the QUARANET framework against standard defense strategies when deployed in asset-constrained environments:

Operational Metric	Conventional Firewalls	Terrestrial Deep Learning	QUARANET V5.1 Framework
Execution Time	Variable (Rule-Dependent)	High Gated Delay	**Deterministic (Constant)**
Memory Behavior	Dynamic Allocation Risks	Extensive Cache Overhead	**Static Framework (Zero Heap)**
Computational Demand	Moderate to High Scaling	Extreme (Requires Hardware Accelerator)	**Minimal (Low Hardware Footprint)**
Environmental Tolerance	Vulnerable to Logic Alterations	Fragile Weight Interdependence	**High Structural Error Invariance**

6. Commercial Framework and TRL Alignment

QUARANET operates under a flexible, highly scalable Intellectual Property (IP) licensing model. Built completely as a hardware-independent firmware block, the solution integrates smoothly across broad embedded avionics architectures, including fault-tolerant ARM, space-certified processing environments, and modern RISC-V computing platforms.

The technology has successfully completed high-fidelity Software-in-the-Loop validation, verifying architecture integrity against simulated communication streams. Ongoing development goals center on migrating the micro-kernel structures toward direct logic synthesis tools, ensuring hardware-in-the-loop laboratory accreditation and mission readiness. The ultimate objective is providing decentralized, cooperative network protection across evolving mega-constellations, establishing a resilient layer of computational safety natively in orbit.