UNIBAP
SPACE SOLUTIONS

UNIBAP SEQR

Unibap SEQR
Built-in security and resilience

Unibap SEQR is our proprietary cybersecurity suite. It secures both the platform and the data that flows through it with a hardware-based chain of trust from data ingestion to applications. Secure boot, signed updates, access control, logging, and tamper detection protect against unauthorized changes. Hardware-rooted keys, signing, and encryption secure data across its lifecycle, while alignment with major standards supports compliance and long-term security.

SECURE PLATFORM

Establishes a hardware-backed chain of trust spanning boot, operation, updates, and recovery to protect mission-critical computing platforms.

- Root of Trust from boot to application
- Zero-trust system architecture
- Secure updates and recovery
- Tamper detection and audit logging
- Protected memory, storage, and interfaces

SECURE DATA

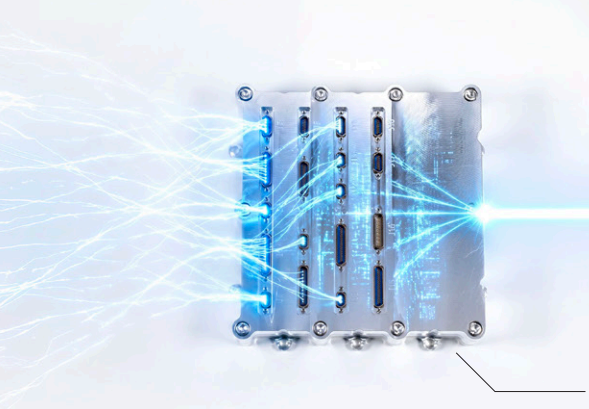
Protects mission data with encryption, signing, and hardware-rooted key management, ensuring confidentiality and integrity from collection to delivery.

- Hardware-rooted cryptographic keys
- Source data signing
- Enabled end-to-end encryption
- High-speed crypto acceleration
- Proven data authenticity and integrity

SECURE ORGANIZATION

Developed and maintained through cybersecurity processes aligned with leading international standards, regulations, and assurance frameworks.

- Secure development and delivery processes
- Alignment with leading cybersecurity frameworks
- Supports CRA, ISO 27001, NIST and CMMC 1 & 2 requirements
- Continuous cybersecurity governance
- Designed for long-term assurance and trust



Just Get the Answer.

Actionable insights from space for critical decisions on Earth.

Next-gen platform
Unibap iX20

Unibap SEQR
Technical specifications

Preliminary information. Specifications subject to change.

PLATFORM SECURITY	
Layered Secure Boot Chain	FPGA → UEFI/BIOS → Kernel
Hardware Root of Trust	FPGA eFuse based AES and ESA/ECDSA keys. AMD fTPM secure boot
Zero Trust	APU/OS isolated from FPGA; only allows signed updates for critical FPGA functionality
Compartmentalization	AppArmor MAC enforcement, per-channel SDMA permissions
Memory & Disk Encryption	TSME encrypts DDR transparently, disk encryption keys are held in fTPM
Tamper-Proof Audit Logging	Security events flow APU → FPGA → MRAM in AES-GCM sealed slots
Secure OTA Update & Recovery	Signed updates with ZFS rollback
OS & Service Hardening	DISA-STIG compliance, systemd sandboxing of all services

DATA SECURITY	
FPGA Source Data Signing	Sensor data signed in the FPGA before reaching the APU, and/or signed in APU after pre-processing by Unibap LOOM
In-Stream Downlink Encryption	Real-time FPGA AES-GCM encryption on data streams
FPGA AES-GCM Crypto Engine	In-fabric signing and encryption without key exposure
High-Throughput SHA-3 Hashing	Hashing at 100 Gbps+ for data integrity verification
APU AES-NI Acceleration	>40 GB/s AES-256-GCM encryption throughput
Post-Quantum Cryptography Support	ML-KEM-1024 key exchange
Active Key Zeroization	Trigger for instant wipe of all plaintext operational keys
Ground-to-FPGA Signed Configuration	Ground-signing of configuration changes that alter critical platform configuration
Encrypted Audit Log Export	Sealed MRAM log slots exported directly with per-entry authentication