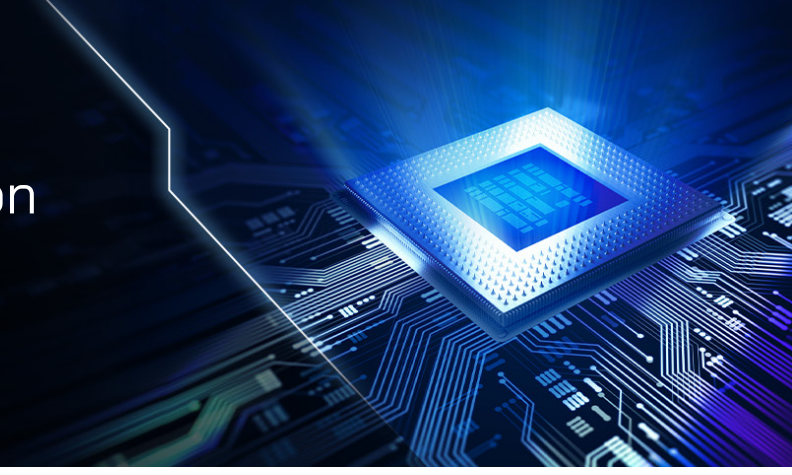


Missile Defense Modernization and Edge Architecture



Executive Overview

Missile defense systems operate under extremely tight decision timelines. Radar sensors must detect and track incoming threats, AI algorithms assist with classification and prioritization, and interceptor guidance systems must execute defensive actions in real time. These capabilities depend on highly reliable and deterministic computing platforms capable of processing large volumes of sensor data at the mission-critical edge.

Drivers of Missile Defense Edge Architecture

Strategic Drivers

- Layered air and missile defense expansion
- Hypersonic and drone threats
- Multi-theater engagement
- NATO interoperability requirements

Lynx Alignment

- Real-time sensor fusion
- Deterministic track-to-intercept loops
- High-assurance GPU acceleration
- Mixed-criticality

Operational Requirements

- Real-time sensor fusion
- Deterministic track-to-intercept loops
- High-assurance GPU acceleration
- Mixed-criticality

Optional Requirements

Modern missile defense systems must support several key functions simultaneously. Sensor fusion algorithms combine radar, satellite, and ISR data streams to create an accurate operational picture. AI analytics help identify and prioritize threats. Command systems coordinate responses across distributed defense networks. All of these functions must operate under strict timing constraints to support track-to-intercept decision loops.



Edge Computing Challenges

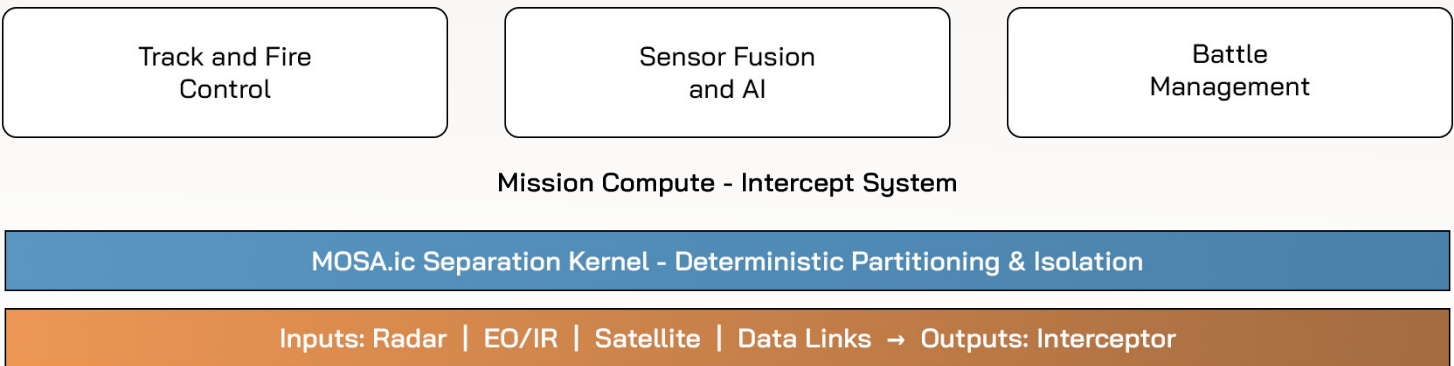
These requirements create several architectural challenges.

Systems must process large volumes of sensor data while maintaining deterministic behavior for safety-critical functions. AI workloads require high-performance compute acceleration, while mission applications must communicate securely with external command networks. At the same time, cybersecurity and safety requirements demand strict isolation between system domains.

Edge Architecture Model

A modern missile defense mission computer typically includes several key domains.

Safety-critical fire control software runs within deterministic real-time partitions. AI-accelerated sensor fusion operates within GPU-enabled compute domains. Command and battle management applications run within general-purpose operating systems. A separation kernel architecture enforces strict boundaries between these domains while enabling secure communication where required.



Strategic Advantage

This architecture allows missile defense platforms to integrate advanced analytics and AI capabilities without compromising determinism or certification boundaries. As defense systems become more software-defined, mission-critical edge computing will increasingly determine operational effectiveness.

Contact Us

edge@lynx.com

US: 408-979-3900

www.lynx.com

© 2026 Copyright Lynx | The information herein is subject to change at any time after the date of publication. Lynx does not guarantee the accuracy of the information herein beyond the date of publication. All third-party company and product names mentioned, and marks and logos used, are trademarks and/or registered trademarks of their respective owners. Lynx trademarks are the property of Lynx.