Reference Mission Computer Architecture Guide

Executive Summary

Defense platforms are evolving toward highly integrated mission systems that combine real-time control, sensor fusion, AI analytics, and operator visualization. Traditionally, these functions were implemented across separate computing subsystems, often resulting in complex integration, higher SWaP (size, weight, power), and slower technology insertion.

Modern mission systems are increasingly adopting consolidated mission computer architectures capable of supporting mixed-criticality workloads on shared hardware. This approach enables safety-critical control systems, mission applications, and AI workloads to coexist while maintaining strict isolation and deterministic performance.

This guide presents a reference architecture for an AI-ready mission computer, illustrating how separation kernels, partitioned operating systems, and GPU acceleration can support next-generation defense systems.

Architecture Overview

A modern mission computer typically supports multiple domains:

- **Safety-Critical Domain:** This domain runs real-time operating systems responsible for safety-critical functions such as flight control, fire control, and other deterministic workloads. These systems must maintain strict real-time behavior and certification compliance.
- **Mission Applications Domain:** Mission applications typically run in general-purpose operating systems such as Linux. These applications support communications, battle management, mission planning, and data exchange across distributed defense systems.
- **AI / Advanced Analytics Domain:** AI workloads process large volumes of sensor data and may perform functions such as threat classification, anomaly detection, or autonomous decision support. These workloads often leverage GPU acceleration to process data in parallel.
- **Visualization and ISR Domain:** Operator displays, situational awareness dashboards, and ISR visualization pipelines require high-performance graphics processing and low latency.

Partitioning and Deterministic Isolation

To support these domains on a single hardware platform, the architecture relies on separation kernel technology that enforces strict partitioning between workloads.

This approach ensures:

- Deterministic execution
- Strict memory isolation
- Controlled inter-domain communication
- Certification boundary preservation

Each software domain operates independently while sharing underlying hardware resources. defense systems.

Benefits of the Architecture

This architecture enables several key advantages for defense platforms.

First, it significantly reduces hardware complexity by consolidating multiple computing subsystems into a single mission computer.

Second, it enables faster technology insertion. New capabilities such as AI analytics or improved visualization can be integrated without redesigning the entire computing infrastructure.

Third, it improves cybersecurity by reducing system interfaces and enforcing strong partition boundaries between software domains.

Finally, it supports long lifecycle sustainment by enabling incremental software upgrades throughout the platform's operational life.

Applicable Defense Platforms

This reference architecture is applicable to a wide range of defense systems, including:

- Missile defense systems
- ISR platforms
- Autonomous aircraft and vehicles
- Naval combat systems
- Multi-domain command systems

Contact Us

edge@lynx.com
US: 408-979-3900
www.lynx.com

LYNX