LYNX

LYNX MOSA.ic™ Technical Whitepaper

Enabling the Digital Backbone for Next-Generation Modular Open Systems

Executive Overview

Aerospace and defense platforms are entering a new architectural era driven by Modular Open Systems Approach (MOSA) mandates, increasing cybersecurity demands, and the need for faster modernization cycles.

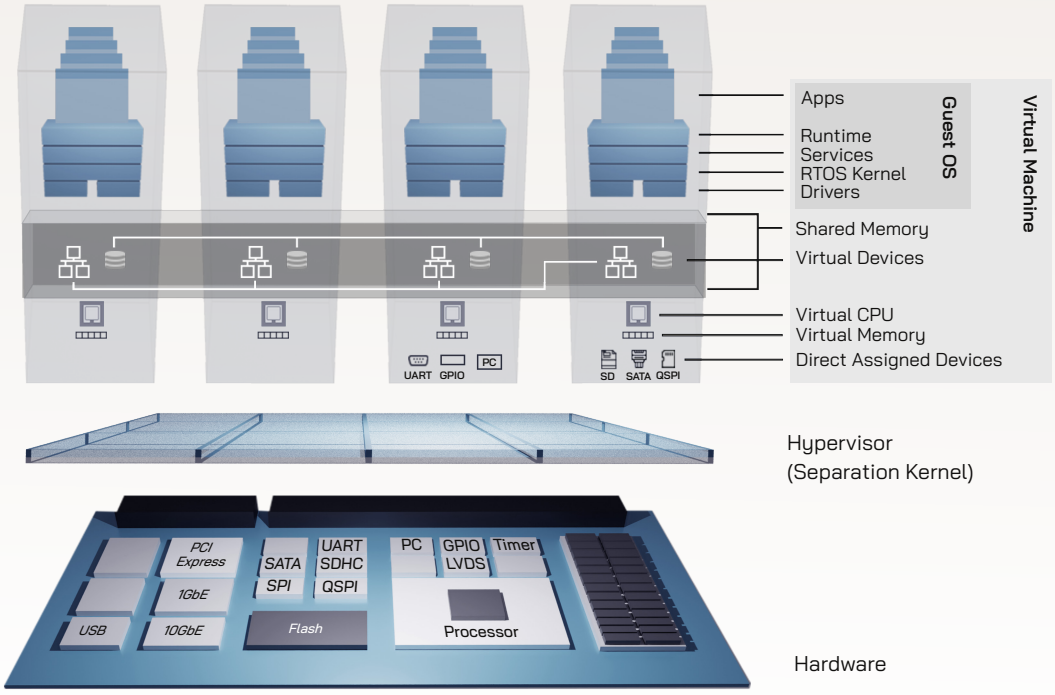
Legacy federated and first-generation IMA architectures were not designed for today's distributed, mixed-criticality, and data-intensive mission environments. Integration complexity, hardware lock-in, and costly upgrades limit long-term agility.

LYNX MOSA.ic introduces a configurable separation-kernel-based digital backplane that enables deterministic compute partitioning, secure device isolation, cross-domain enforcement, and TSN-ready network consolidation within a modular open framework.

MOSA.ic Architecture

- VM Allocations
  - CPU
  - Memory
  - Physical Devices
  - Virtual Devices
  - Time
- System Scheduling
- Permission Management
- Exception Management

Rather than treating integration as a one-time engineering event, MOSA.ic establishes a reusable digital infrastructure foundation that allows platforms to evolve over decades.



The Architectural Inflection Point

Mission systems are shifting from federated boxes and legacy buses to distributed digital backbone architectures. This shift is driven by edge analytics, AI acceleration, cross-domain data flows, and Ethernet/TSN networking.

Traditional integration models cannot scale efficiently under these demands. Programs require composable systems that preserve determinism, enforce security boundaries, and support incremental capability insertion.

The architectural question is no longer how to consolidate compute, but how to consolidate responsibly, without sacrificing assurance, safety, or long-term adaptability. This transition is especially important for unmanned and space systems, where size, weight, power, lifecycle longevity, remote updateability, and secure multi role consolidation place even greater value on deterministic modular architectures.

This transition is especially important for unmanned and space systems, where size, weight, power, lifecycle longevity, remote updateability, and secure multi role consolidation place even greater value on deterministic modular architectures.

A Configurable Digital Backbone

MOSA.ic is built on a separation-kernel hypervisor that enforces strict memory, CPU, and device isolation. Each software subject operates within its own protected execution environment.

Virtual CPUs are deterministically allocated and bound to physical cores. Devices can be directly assigned with hardware enforcement or virtualized through controlled service channels.

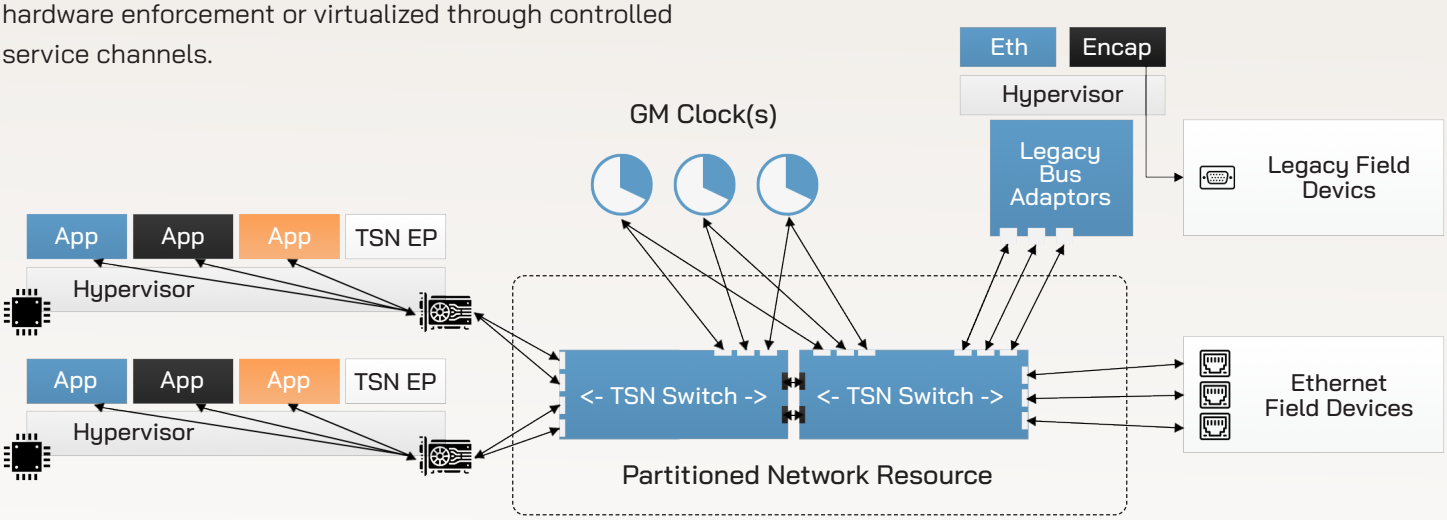
Virtualization to Composition

Data Concentration Unit:

- Encapsulate legacy device data on Ethernet bus

Application Platform

- Deliver heterogeneous data streams to high-capacity compute platform



This structure transforms virtualization into disciplined composition, enabling independent software components to coexist safely on shared hardware.

Deterministic Mixed-Criticality Consolidation

Modern edge platforms are no longer single purpose. They are expected to run safety-critical control logic alongside mission applications, networking stacks, and increasingly AI and analytics workloads, all on shared compute resources.

This convergence creates a fundamental challenge: how to consolidate workloads of different criticality levels without introducing interference, timing unpredictability, or certification risk.

MOSA.ic addresses this by enabling deterministic mixed-criticality consolidation at the platform level.

Through configurable scheduling models and strict resource partitioning, the system ensures that workloads remain pinned, predictable, and isolated, preventing issues such as uncontrolled core migration, resource contention, or timing jitter that can undermine real-time performance.

At the same time, MOSA.ic establishes clear fault containment regions across compute, memory, and I/O. This architectural separation allows each function, whether safety-critical or mission level, to be analyzed, validated, and certified within a well-defined boundary.

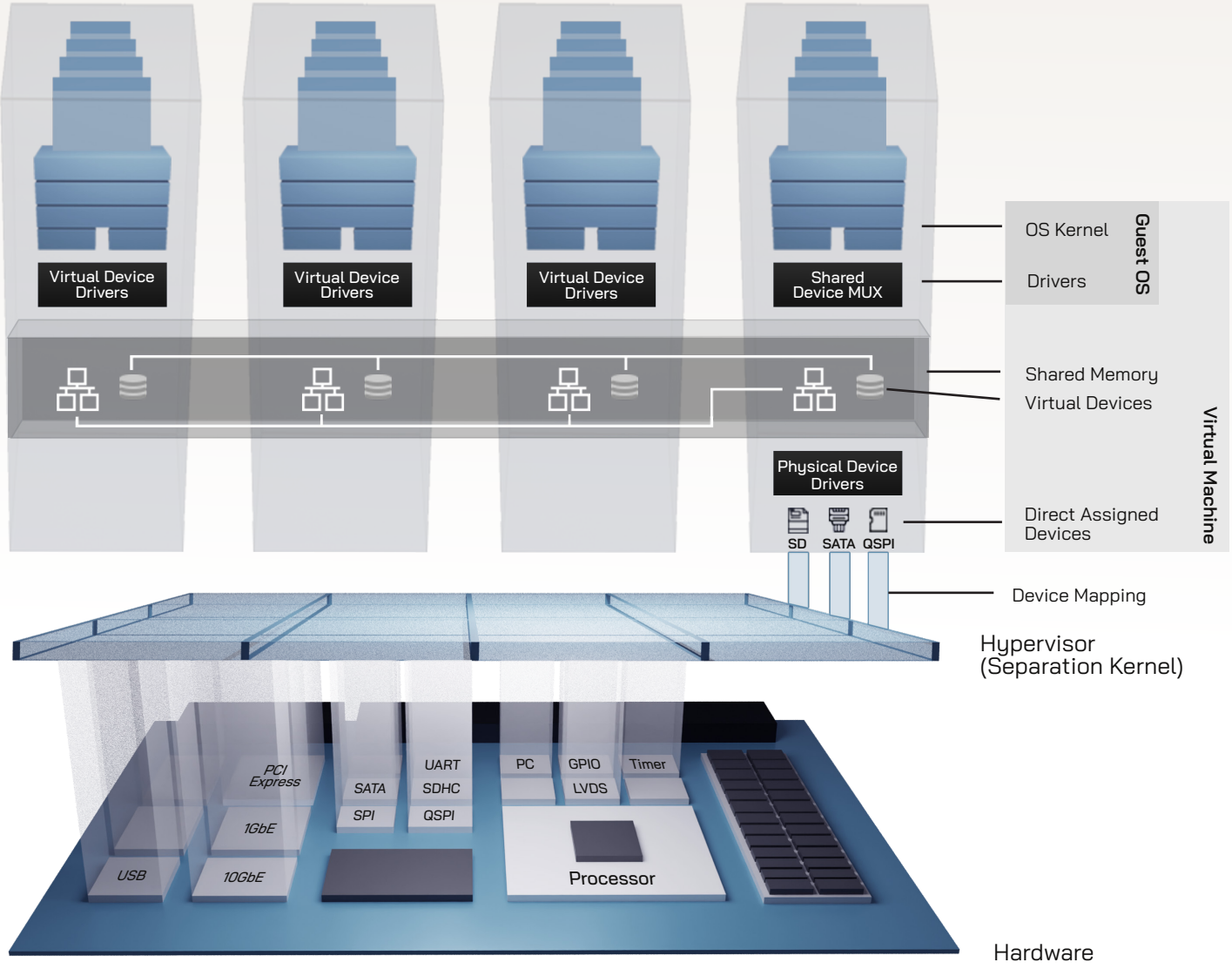
The result is twofold:

- Preserved determinism, even under complex, multi-domain workloads
- Reduced certification scope, enabling faster, more predictable validation cycles

Virtual Device Sharing

Service VM:

- Direct Assigned DMA Device
- Virtual P2P Connections to Applications



By combining consolidation with strict control and isolation, MOSA.ic enables programs to do more on shared hardware without compromising safety, timing guarantees, or assurance requirements.

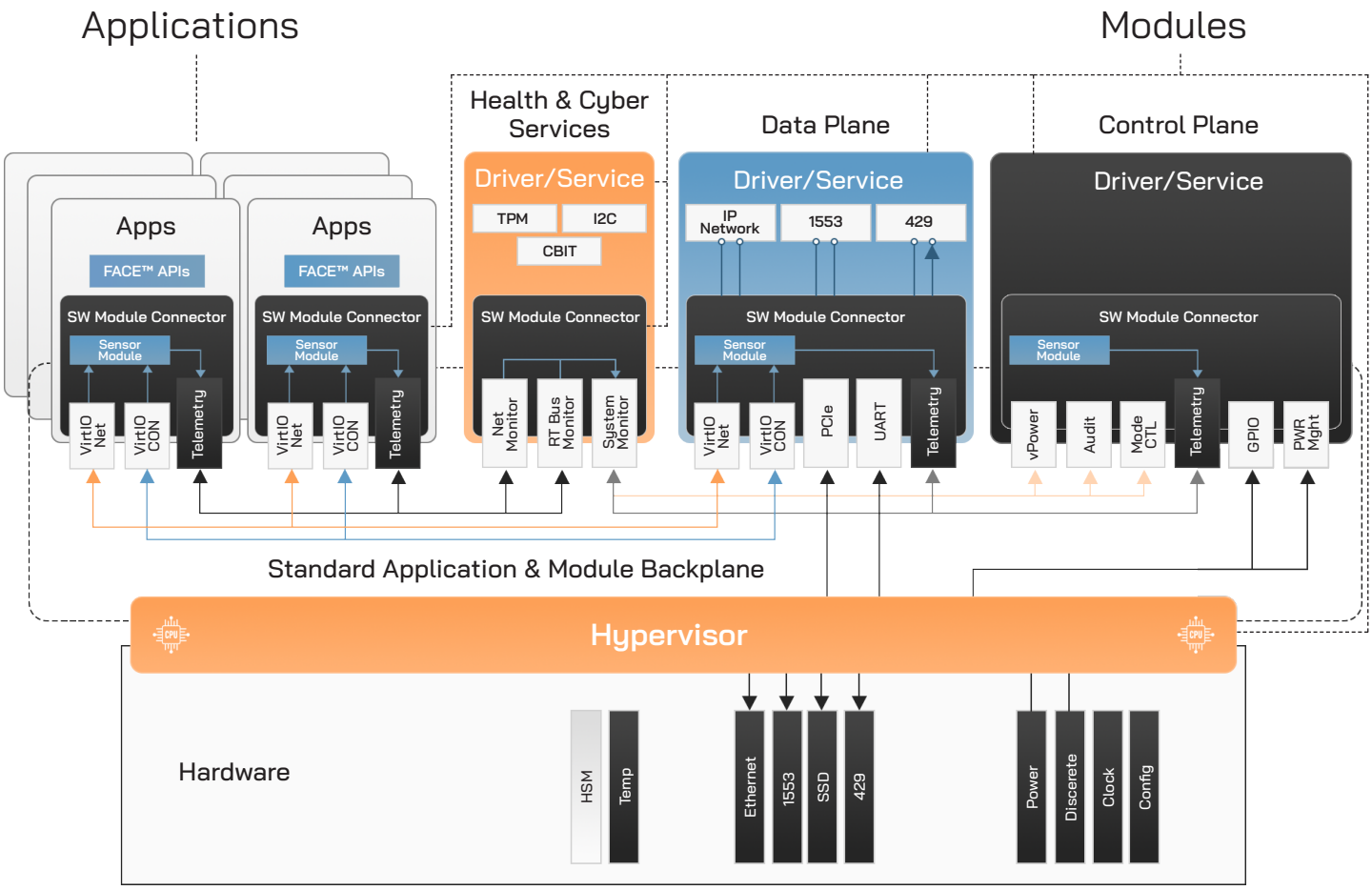
Isolation as the Foundation of Cybersecurity

In modern avionics and mission critical systems, cybersecurity can no longer be treated as an overlay. It must be designed into the architecture from the ground up, where enforcement is intrinsic, not dependent on application behavior. As platforms consolidate multiple functions such as flight control, mission processing, connectivity, and AI workloads, the attack surface expands. Without strong isolation, a vulnerability in one domain can propagate across the system. service channels.

LYNX MOSA.ic addresses this by making isolation the first principle of system design.

At the hardware and system level, the platform enforces IOMMU-based device separation, ensuring that peripherals and accelerators can only access explicitly assigned memory regions. This prevents unauthorized DMA access and limits the blast radius of compromised components. Memory is further secured through strict partitioning and protected address spaces, guaranteeing that applications and services operate within well-defined boundaries. These protections are enforced by the platform, not left to developer discipline.

In addition, MOSA.ic introduces non-bypass monitoring and control services that provide continuous visibility into system behavior. These services act as a trusted layer for enforcing policy, detecting anomalies, and supporting cyber survivability strategies. Crucially, when interaction across domains is required, MOSA.ic enables controlled, policy-driven communication through trusted partitions. These mediation points validate data, enforce protocols, and ensure that information flows only as intended across security boundaries.



The result is a system architecture where:

- Isolation limit's fault and threat propagation
- Access to compute, memory, and devices is explicitly controlled
- Cross-domain interactions are governed, not implicit

By embedding these principles into the platform, MOSA.ic enables organizations to move from reactive security measures to proactive, architecture-driven cybersecurity, aligned with zero trust and designed for long-term assurance.

Digital Backbone & Network Consolidation

A fundamental shift is underway in mission-critical systems: legacy point-to-point buses are giving way to Ethernet and TSN-based architectures that provide higher bandwidth, flexibility, and scalability. However, modernization is rarely a clean break. Most programs must integrate new network paradigms while continuing to support existing protocols, certified subsystems, and long lifecycle platforms.

MOSA.ic enables this transition by acting as a digital backbone that bridges legacy and modern architectures. Through support for protocol encapsulation and translation, legacy data flows can be integrated into Ethernet/TSN networks without requiring immediate redesign of existing subsystems. This allows programs to modernize incrementally, reducing risk and avoiding costly, large-scale system replacements.

At the same time, MOSA.ic enforces partitioned network resource allocation, ensuring that bandwidth, latency, and communication paths remain predictable and aligned with mission requirements. This is critical in environments where network contention or jitter can directly impact system performance or safety.

By combining deterministic networking with compute consolidation, the platform enables multi-role hardware reuse. A single platform can be configured, rather than redesigned, to operate as:

- A data concentrator, aggregating and normalizing inputs from multiple subsystems
- An edge compute node, processing data locally for real-time decision-making
- A cross-domain gateway, enforcing controlled data exchange across security boundaries

This flexibility transforms hardware from fixed-function components into adaptive infrastructure, capable of evolving with mission needs.

The result is a network and compute architecture that:

- Supports gradual, low-risk modernization
- Maintains determinism and control over network behavior
- Maximizes reuse of hardware across multiple roles and programs

By establishing a unified digital backbone, MOSA.ic enables organizations to modernize at their own pace while building toward a scalable, software-defined future.

Composable System Roles

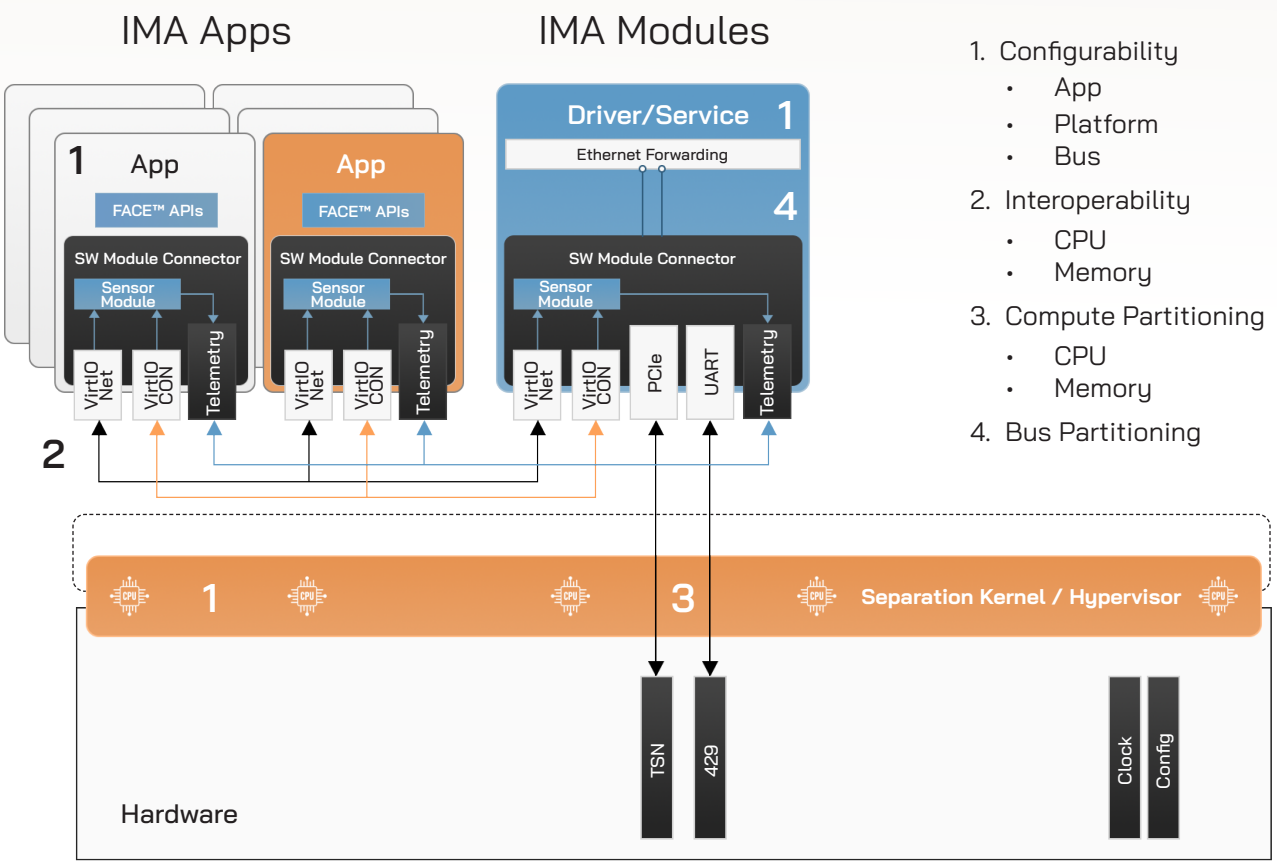
Modern mission systems are evolving toward greater flexibility, but traditional architectures still rely on fixed-function hardware, where each component is designed, integrated, and certified for a single role. This approach increases non-recurring engineering (NRE), limits reuse and slows adaptation to new mission needs.

MOSA.ic shifts this model by enabling composable system roles, where a single hardware platform can be configured to perform multiple functions across programs and domains.

Depending on mission requirements, the same platform can operate as a:

- Compute module for mission applications
- Sensor processor for data acquisition and pre-processing
- Network node within a distributed system architecture
- Secure gateway enforcing cross-domain data exchange
- Unmanned mission processor for autonomous systems
- Edge compute node for space and distributed operations

This flexibility is enabled through software-defined configuration, not hardware redesign. Applications, services, and system behaviors are assembled using standardized interfaces, APIs, and modular components, allowing capabilities to be composed, updated, or repurposed over time.



At the platform level, MOSA.ic enforces resource partitioning across CPU, memory, and I/O, ensuring that even as roles change, system behavior remains deterministic and aligned with mission and certification requirements.

The impact is significant:

- Reduced NRE and integration effort through reuse of common hardware platforms
- Faster deployment cycles, as new roles are enabled through configuration rather than redesign
- Greater lifecycle adaptability, allowing systems to evolve with mission needs
- Consistent certification approach, even across different deployments

By decoupling function from hardware, MOSA.ic enables a shift toward software-defined, reusable infrastructure, where systems are no longer built for a single purpose but designed to adapt across missions, programs, and operational environments.

Reducing Lifecycle Risk

For most mission-critical systems, most cost and risk does not come from initial development, but from decades of sustainment, upgrades, and technology refresh cycles.

Traditional architectures tightly couple applications to specific hardware platforms and software environments. As a result, even small changes can trigger broad revalidation efforts, regression risk, and costly redesigns, slowing modernization and increasing total program cost.

MOSA.ic addresses this by enforcing a clear separation between applications and underlying hardware dependencies.

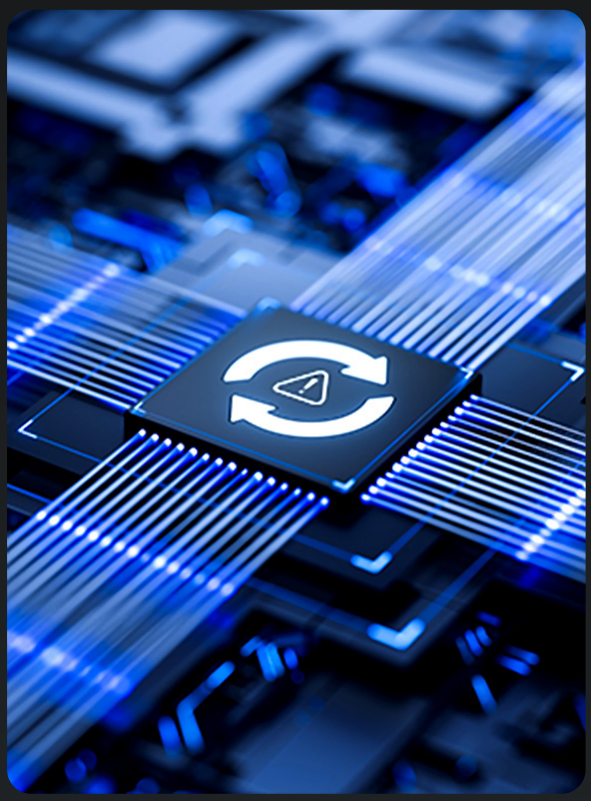
Through virtualization, partitioning, and stable platform interfaces, applications can be deployed within well-defined, isolated environments that remain consistent, even as hardware evolves. This allows new capabilities to be introduced in new or modified partitions without impacting existing, certified functions.

Critically, this approach preserves system integrity while enabling incremental modernization. Instead of large, disruptive upgrades, programs can evolve step by step, adding functionality, updating components, or integrating new technologies such as AI, without destabilizing the overall system.

The benefits are substantial:

- Reduced lifecycle risk, by limiting the scope of change and revalidation
- Shorter modernization cycles, enabling faster deployment of new capabilities
- Lower regression risk, as certified functions remain isolated and unaffected
- Extended platform longevity, maximizing return on existing investments

By decoupling application evolution from hardware refresh cycles, MOSA.ic enables a shift from periodic, high-risk upgrades to continuous, controlled modernization, aligned with the long operational lifetimes of aerospace, defense, and industrial systems.



Alignment with MOSA Principles

Modern mission systems demand openness to integrate best-of-breed technologies, avoid vendor lock-in, and support evolving ecosystems. But in safety- and security-critical environments, openness without control introduces risk: unbounded interactions, loss of isolation, and increased certification complexity.

LYNX MOSA.ic is designed to resolve this tension by combining open interfaces with enforced architectural control.

The platform adopts standard APIs and well-defined communication mechanisms, enabling interoperability across applications, middleware, and hardware components. This allows programs to integrate third-party technologies, reuse existing assets, and evolve systems over time without being constrained by proprietary stacks.

At the same time, MOSA.ic enforces strict separation boundaries across compute, memory, and I/O domains. All interactions between components are mediated through controlled interfaces, ensuring that openness does not translate into uncontrolled access or unintended coupling.

This approach enables composable integration, where components can interoperate through standard mechanisms, while remaining isolated, predictable, and certifiable within their respective domains.

The result is a balanced architecture that:

- Enables interoperability and ecosystem flexibility through open standards
- Maintains control over system behavior through enforced isolation and partitioning
- Supports certification and assurance processes by clearly defining interaction boundaries
- Allows long-term evolution, as components can be updated or replaced without destabilizing the system

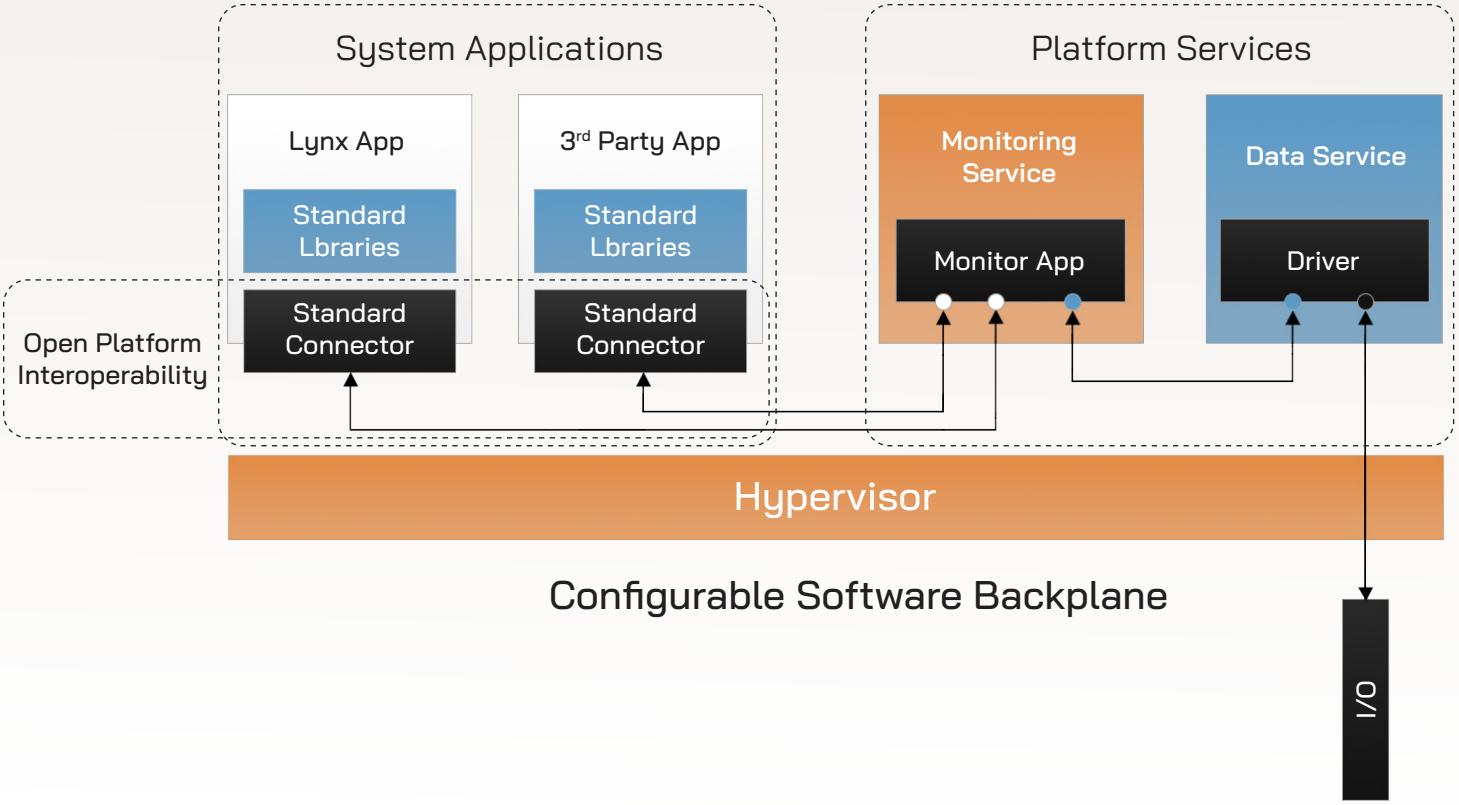
By bridging openness with control, MOSA.ic provides a foundation for sustainable, modular system architectures, where innovation can be integrated continuously, without compromising safety, security, or system integrity.

Conclusion

Next-generation aerospace, defense, unmanned, and space systems are no longer defined by individual components, but by the architecture that enables them to evolve.

These systems must be composable, secure, and adaptable by design, capable of integrating new technologies, supporting mixed-criticality workloads, and scaling across missions, without compromising safety, determinism, or certification integrity. MOSA.ic provides this foundation.

By combining separation-kernel enforcement, deterministic partitioning, secure device isolation, and a unified digital backbone, the platform establishes a configurable software-defined infrastructure that brings control to complexity.



It enables organizations to:

- Control system behavior through enforced isolation and deterministic execution
- Enable integration of diverse workloads, from legacy functions to AI-driven applications
- Govern lifecycle evolution with clear boundaries that support certification and long-term sustainment

Rather than treating modernization, cybersecurity, and interoperability as separate challenges, MOSA.ic integrates them into a cohesive architectural approach.

The result is a platform that does not just support today's requirements—but provides a durable foundation for continuous evolution, aligned with the principles of modular open systems and the realities of long-lived mission-critical programs.

Ready to Revolutionalize Your Mission-Critical Systems?

Contact Lynx today to learn more about how LYNX MOSA.ic can empower your success and help you Seize the Edge in every mission-critical endeavor

edge@lynx.com

www.lynx.com