LYNX MOSA.ic™

Research shows that 31% of cost overruns result from insufficient analysis of systems requirements and underestimating technology complexity in early stages of planning. Getting the design right from day one drastically reduces these costs. *Source: Defense Acquisition University, Mckinsey.* LYNX MOSA.ic™ helps you achieve this.

Modular Operating Environment Designed for Multicore Systems to Host Highly Safe and Secure Applications

In traditional multicore systems, managing the integration of diverse, safety-critical applications leads to increased complexity, extended development cycles, and skyrocketing certification costs. Existing Real-Time Operating Systems (RTOS) stack all system services: hardware control, real-time scheduling, security, and multimedia into a single, monolithic architecture, creating challenges in flexibility, scalability, and security. This hinders the ability to meet rigorous safety and certification standards, complicates debugging, and slows down system integration.

LYNX MOSA.ic revolutionizes this approach by allowing system architects to create smaller, independent stacks, tailored to each application's needs. LYNX MOSA.ic is a software development framework for building comprehensible software systems from just such independent application modules, delivering the Modular Open Systems Approach (MOSA) vision. LYNX MOSA.ic enables developers to collapse existing development cycles to create, certify, and deploy robust, secure, mission-critical platforms. Acting as an Integration Center – this is the ".ic" in LYNX MOSA.ic – it streamlines the integration of independent application modules. With unified tools and frameworks, LYNX MOSA.ic simplifies the management and integration of diverse software components, even in complex multicore environments, reducing complexity and accelerating development cycles.

Customer Adoption of LYNX MOSA.ic

LYNX MOSA.ic is the foundational software technology powering a wide range of safety-critical platforms, ensuring unmatched reliability and performance. One customer reported that our architecture eliminated the need for hundreds of thousands of lines of code and reduced certification costs by tens of millions of dollars. Publicly disclosed programs harnessing LYNX MOSA.ic include:

Lockheed Martin F-35

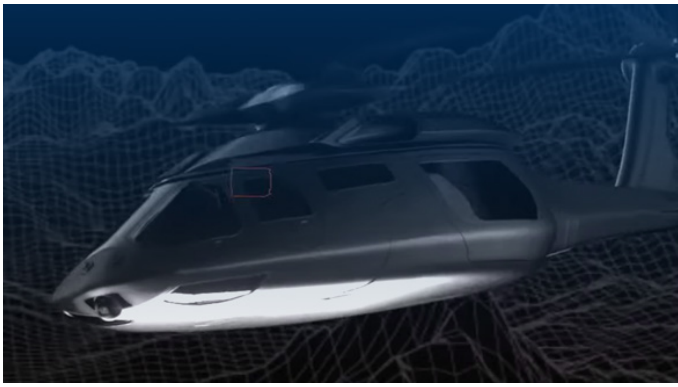
LYNX MOSA.ic powers the Panoramic Cockpit Display (PCD) and Integrated Core Processor (ICP) avionics platforms. Customers highlighted the streamlined development process for migrating software from Linux to the LynxOS-178 real-time operating system. LYNX MOSA.ic was instrumental in achieving F-35 SEAL Level 1, equivalent to DO-178C DAL A.

General Atomics Gray Eagle Extended Range Uncrewed Aerial System (UAS)

This Arm-based (Xilinx MPSoC) architecture leveraged LYNX MOSA.ic to transform a mixed criticality system (Linux and LynxOS-178) from what was previously a monolithic stack.

Collins Perigon

The mission computer in this system supports bare metal applications on LynxSecure, the foundational separation kernel in LYNX MOSA.ic, across three processor architectures.



LYNX
SOFTWARE TECHNOLOGIES

LYNX MOSA.ic Customer Benefits

Customer Benefits	Capability Enabled by LYNX MOSA.ic
Enhanced Safety and Security as Priceless Value	LYNX MOSA.ic delivers systems purpose-built for safety and security, ensuring that customers can rely on robust, multi-core platforms designed from the ground up to meet the highest certification standards. This enables the development of highly reliable, high-performance systems that are critical in industries like aerospace, defense, and automotive.
Optimized Multi-Core Performance by reducing overhead by 25% *Source: Lynx internal report*	By leveraging an architecture natively designed for multi-core environments, Lynx MOSA.ic offers unmatched efficiency and scalability. Customers benefit from streamlined development processes and improved performance, while avoiding the limitations of retrofitted single-core systems and gaining the flexibility to scale operations more effectively.
Lower Certification Costs with 30% of eLOC count. *Source: Lynx internal report*	MOSA.ic's modular, multi-core architecture significantly reduces certification costs by streamlining the adaptation of legacy single-core designs to modern multi-core systems. This allows customers to achieve certifications faster and more cost-effectively, speeding up time-to-market while maintaining compliance with regulatory requirements.

LynxSecure Hypervisor Simplifies Multi-Core RTOS with Enhanced Partitioning and Portability

RTOS applications are built as virtual machines partitioned by a separation kernel hypervisor. The use of LynxSecure, Lynx's separation kernel, addresses the complexity challenges of building multi-core systems that must conform to reference architecture standards while providing greater platform robustness and application portability properties over conventional RTOS design.

LynxSecure's primary role is to partition, allocate, and arbitrate access to physical resources. It is developed according to DO-178C DAL A software development standards and supports ARINC 653 architecture requirements. The lightweight hypervisor primarily serves as a hardware control plane for the overall system. The hypervisor does not provide application or data services. All resource allocation and policy enforcement capabilities provided by the hypervisor apply to the definition of virtual machines and their assigned resource and access control permissions. This approach creates a hardware-enforced software architecture for a given system configuration.

LYNX MOSA.ic Architecture and Runtime: Control & Data Plane Integration on LRU Processing Board

The figures below illustrate an example of LYNX MOSA.ic on a LRU processing board. The runtime architecture consists of two core platform technologies:

- **Control Plane** - Multicore hardware time and space separation, managed by a separation kernel hypervisor
- **Data Plane** – Guest operating system and application development tools for building Real-time POSIX and ARINC applications within VMs

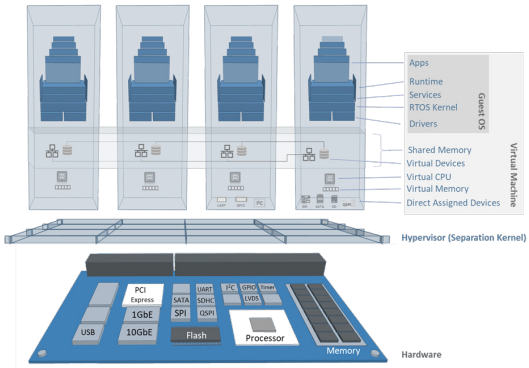


Figure 1 - LYNX MOSA.ic™ Platform Composition Overview

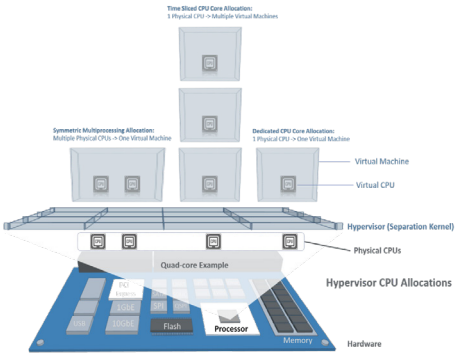


Figure 2 - Hypervisor CPU Allocation

Key Capabilities

Multi-core Support

The hypervisor permits the flexible allocation of CPU cores to virtual machine environments. The graphic on the previous page illustrates the flexibility of hosting various execution configurations simultaneously.

Flexible Scheduling Support

When allocating a physical CPU shared by multiple virtual machines, the hypervisor offers configurable options to schedule virtual machines contexts:

- **Tickless Scheduler -** An optional feature in LYNX MOSA.ic, the tickless scheduler enhances determinism, reliability, and efficiency in mission-critical real-time systems by eliminating periodic timer ticks, reducing context switches, and adapting to varying workloads
- **Static Cyclic –** Each virtual machine is assigned an execution duration and cyclic period following ARINC 653 time partitioning standards
- **Static/Adaptive Cyclic –** Multiple static execution policies may be defined with different duration and period parameters per virtual machine
- **Priority Preemptive –** Virtual CPUs allocated to virtual machines are assigned priorities, which function as threads to apriority pre-emptive scheduler within the hypervisor
- **Aperiodic Reservation** – Virtual CPUs may be designated for hosting sporadic workloads and are guaranteed a user defined budget of execution time per major frame
- **Co-operative "Z-Scheduling"** – Context switching capability can be delegated to a VM, allowing it to control context switching with conditional and bounded execution periods granted by the hypervisor

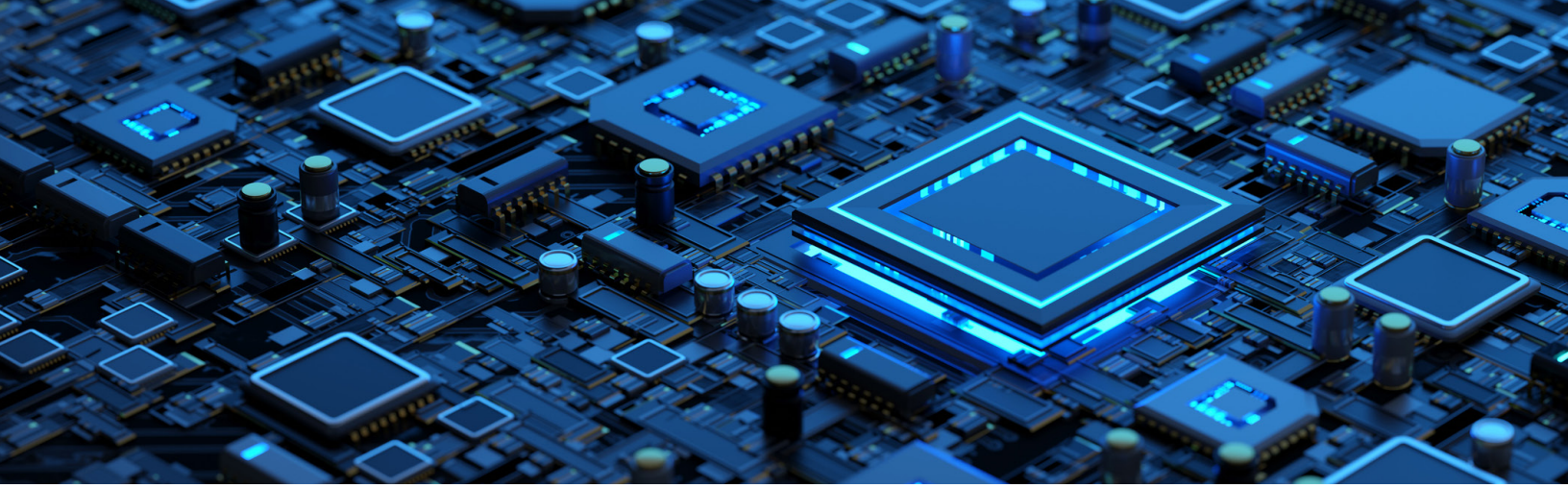
Virtual Device Emulation

The hypervisor can allocate peripheral interfaces to virtual machines that are not directly mapped to physical hardware. Virtual devices are commonly used to facilitate inter-VM communication and to multiplex the use of physical devices. Device virtualization is a foundational feature that allows RTOS runtimes to utilize the POSIX file system and networking features across all CPU cores.

Lynx's CDK includes Support to Build the Following Guest Software Types

- **Bare-metal (LSA) –** Main C program, supported by 64-bit C libraries and GCC toolchain to build simple applications with minimal runtime complexity
- **RTOS (LynxOS-178)** – Safety certified, preemptive hard real-time operating system. Provides multi-process, multi-threaded POSIX and ARINC runtime services and hard real-time scheduling primitives
- **Unikernel (LynxElement) -** A consolidated multi-threaded, single-process RTOS environment that removes redundant architectural constructs shared between the RTOS guest kernel and separation kernels. Unikernel applications are provided standard ARINC and POSIX libraries and a fully featured stack
- **Linux (Buildroot) –** Lightweight embedded Linux toolchain. Provides broad peripheral support using native Linux kernel.org kernel images. Buildroot provides customization tools to select kernel modules and application packages to include in RAM disk and boot images

A virtual machine may also host guest software 3rd party binary OS distributions for example: Windows, Red Hat, Ubuntu, etc.



FACE® Version 3.1 64-Bit Industry Standard Conformance

The Future Airborne Capability Environment (FACE®) Technical Standard is designed to enhance software reuse, accelerate warfighter capabilities, and drive the adoption of new technologies within U.S. military aviation. The FACE Consortium, comprising of industry and government members, provides a neutral platform for collaboration, enabling the development of open standards and influencing procurement and policy decisions.

As an Associate Sponsor of the FACE Consortium, Lynx Software Technologies contributes to the framework that defines a common operating environment, supporting applications across multiple Department of Defense avionics systems. LynxOS-178® has been certified conformant to version 3.1 of the FACE Technical Standard as an Operating System Segment (OSS) meeting the Safety Extended Profile for 64-bit Arm, and Intel® x86 processors.

Virtual Integration Environment + Embedded Board Farm Integration

Lynx offers the Virtual Integration Environment (VIE), a platform that enables teams to develop, test, and debug software on virtual hardware before physical boards are available. Now integrated with Embedded Board Farm (EBF), VIE provides seamless testing on both virtual and physical environments. EBF offers remote access to live hardware, managing tasks like power control, USB hot-plugging, and network management. This combined solution enables continuous integration, remote debugging, and automated testing, enhancing collaboration and reducing reliance on physical hardware, all within a secure and efficient framework.

LYNX MOSA.ic.SCA

LYNX MOSA,ic now includes an Software Bill of Materials (SBOM) representative of the specific version of MOSA.ic. In addition, LYNX MOSA.ic offers an add-on product to dynamically manage Software Composition Analysis (SCA) capability to address cybersecurity and transparency needs in regulated industries like military and avionics. This solution simplifies compliance with mandates such as White House EO 14028, offers full component transparency, and integrates with CI/CD pipelines. It supports formats including CycloneDX and SPDX, and features tools for CVE tracking, patch management, and risk prioritization, streamlining security management throughout development and deployment.

Lynx Partners Providing Complementary Technology

Systems continue to increase in complexity at a time when there has never been a stronger focus on improving development timescales. Lynx works closely with a diverse set of partners (see below) to prove our technology works optimally with LYNX MOSA.ic. Lynx is increasingly focused on ensuring MOSA.ic is the Integration Center of future systems. Consequently, we partner with best-in-class third-party technologies providers to enhance Lynx MOSA.ic.

RunSafe Security™

Lynx MOSA.ic is designed to offer robust protection against threats by minimizing attack surfaces. To further enhance security, MOSA.ic integrates with RunSafe Code™, a solution developed with Lynx partner RunSafe Security. Based on the DoD-proven Runtime Application Self-Protection (RASP) approach, RunSafe Code addresses the security gaps left by traditional scanning and patching methods.

RunSafe Code mitigates vulnerabilities such as buffer and heap overflows, which account for 70% of all exploits, by rendering any information gathered during an attack unusable.

Source: Chromium Project. "Memory Safety." Chromium Security. Accessed September 14, 2024. https://www.chromium.org/Home/chromium-security/memory-safety/

RunSafe Code protection also provides fine-grained Address Space Layout Randomization (ASLR), relocating functions in memory at runtime while maintaining real-time performance guarantees for the RTOS. The RunSafe solution is set to be certified under DO-330 TQL-1 for tools and DAL A for runtime.

SpyKer TZ Powered by Percepio®

Lynx SpyKer-TZ, powered by Percepio Tracealyzer technology, is an advanced trace analysis tool integrated with LYNX MOSA.ic that enhances observability and debugging capabilities. It offers detailed insights into program execution, enabling profiling, debugging, and system-level analysis. SpyKer-TZ facilitates real-time, non-intrusive event tracing, supporting various views, including trace, CPU load graphs, and event logs. These features allow developers to identify performance issues, optimize system behavior, and ensure efficient resource usage across safety-critical applications. Spyker-TZ supports both a rich user interface and deployment into the customer software pipeline for CI/CD.

LYNX PARTNER ECOSYSTEM