Joint Strike Fighter (F-35)



Collins Aerospace Perigon



General Atomics (Gray Eagle)

## Company Background

Thirty four year old US company with two+ decades in supporting customers in the creation of highly complex mission critical platforms for military, aerospace and federal applications.

Lynx was acquired in June 2022 by OceanSound Partners ("OceanSound"), a New York-based private equity firm that invests in technology and technology-enabled services companies serving government and enterprise end-markets.

The result of this strong financial backing, coupled with the arrival of Tim Reed as the company's new CEO, provides the opportunity to extend the value of technology that Lynx delivers to these same markets.

# LYNX
## SOFTWARE TECHNOLOGIES

# Software Platform For Highly Secure, Mission Critical Edge Applications

### Relevant Industry Challenges

Simply put, the creators of the next generation of military, aerospace and federal platforms are being challenged to deliver more functionality in tighter time, cost and power budgets while ensuring existing levels of system robustness and resiliency are met.

Across market segments, "black boxes" are evolving to become connected "systems of systems" which require high (and continued rising levels over time) immunity to compromise, flexibility to adapt to evolving needs and architectures that avoid vendor lock in.

At the heart of these systems are heterogenous, massively multicore processors, many of which were initially defined with less safety-stringent use cases in mind.
Harnessing these processors in mission critical computers for (increasingly autonomous) military aircraft, helicopters and drones requires software frameworks that
- Guarantee real-time responses to events no matter what else is being processed by the systems
- Maintain high levels of system security and robustness when multiple safety-critical and general-purpose applications are running concurrently
- Provide a cost-, time- and low risk-path to rigorous safety certification standards in the face of spiraling system complexity

### Lynx Software Technologies (Lynx)

Today, software technology from Lynx Software Technologies (Lynx) powers some of the most complex commercial and military platforms that keep humans safe and secure. The LYNX MOSA.ic software framework incorporates the unique and highly secure separation kernel hypervisor (LynxSecure), operating systems and management technologies that layer directly on top of the most popular processor architectures (Intel, ARM and PowerPC). Customers benefit from;
- A software framework that allows Lynx, 3rd party (including competitor's technology) and customer-developed software to be embraced, harmonized and codified into platforms
- Updatable systems that can deliver predictable, real-time (10s of microseconds) responses to events and provide virtual air-gapping to run custom, container based and open-source workloads without compromising security and/or safety
- Lynx's extensive experience with the industry's most stringent military (SEAL) and commercial DO178C DAL A system certifications

Our value proposition and product portfolio going forward is driven by the company's mission to improve the economics to our customers and ecosystem partners to design, develop, deploy and service high-assurance edge applications through innovative, modular, and open standard solutions.

## Product Overview

The LYNX MOSA.ic™ development framework is a composite CDK including cross-development and integration tools for building RTOS applications as virtual machine partitions to run on a separation kernel hypervisor. The separation kernel approach offers greater benefits in terms of platform robustness and application portability properties over an SMP RTOS.

The figure to the right shows the flexibility of technologies that can be reliably combined using the LYNX MOSA.ic software framework to run on advanced multi-ticore processors from a variety of suppliers. System architects can (immutably) configure virtual machines (VM) that host general-purpose (Windows or Linux) applications, hard real-time applications and high speed DMA device drivers and device sharing services. LynxSecure, the separation kernel hypervisor, guarantees that the impact of hazardous events such as erroneous DMA and interrupt pre-emption is constrained to the VM assigned to the device, protecting the integrity and timing of the other VMs. Lynx also provides connectivity to a number of cloud services, enabling the support of container technologies and connectivity to customer-proprietary and 3rd party orchestration software The hypervisor guarantees that the impact of hazardous events such as erroneous DMA and interrupt pre-emption is constrained to the VM assigned to the device, protecting the integrity and timing of the other VMs.
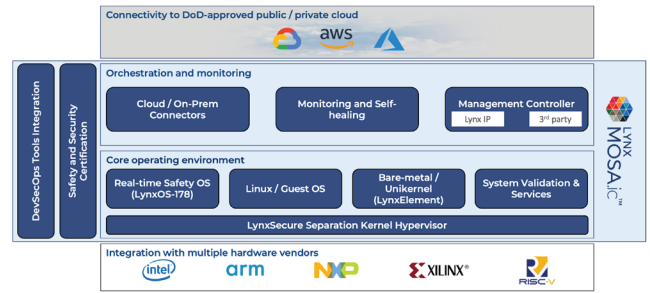
## System Benefits

In contrast to a traditional RTOS platform, where all hardware control, real-time scheduling, security, and application runtime services are integrated into a common stack, LYNX MOSA.ic™ allows system architects to subdivide systems into smaller independent stacks. These only include the runtime dependencies needed per application.
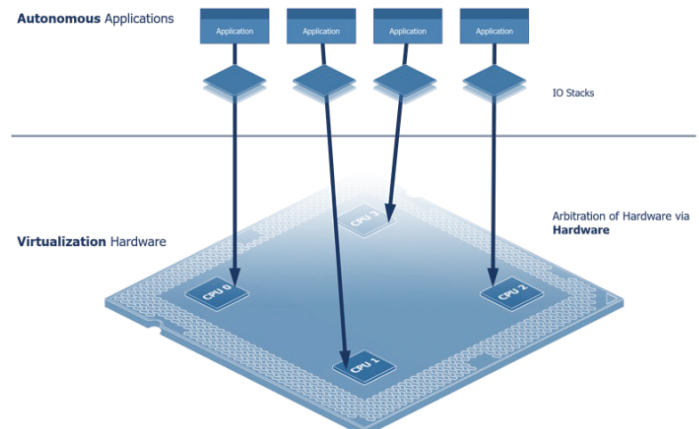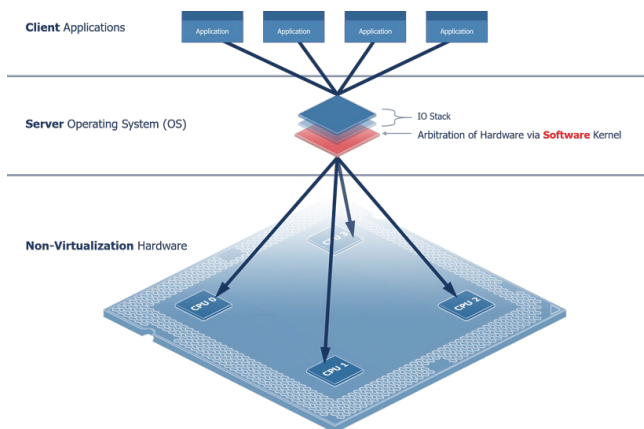
Prior to CPU virtualization, operating systems (general-purpose OSes or RTOSes) forced a centralized client-server model of execution behavior, wherein each user application is a client to an OS server that arbitrates the use of physical resources.

The approach of stack separation drastically reduces software complexity which provides the following benefits;

1. Promoting comprehensible tracible architectures
2. Improving formalism of system composition to aid security and safety analysis
3. Reducing time to debug
4. Increasing the speed of system integration

This approach immediately reduces the need to context switch, copy, or share data—unlocking higher performance thresholds, better timing control, and improved modular properties such as rapid development & testing, component reuse, and design refactoring.

LYNX MOSA.ic™ simplifies vital platform abstraction layers—isolating computing resources into independent distributed environments which are uniquely capable of managing themselves. The comprehensible, hardware -enforced architecture makes inherently complex multi-core system development a viable option when facing the risks of building solutions in highly regulated safety- and security- conscious markets.