LYNX
SOFTWARE TECHNOLOGIES

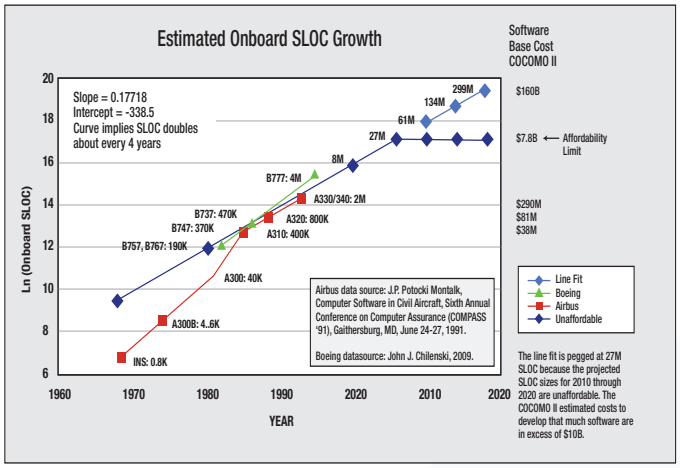
Proven track record in delivering leadership software technologies for mission critical systems

Product line directors of equipment that need to be deployed and continue to contribute value for greater than ten years have never been more challenged than they are in 2020

- How do they nimbly adjust to mitigate acquisitions, companies going bankrupt and government mandates about what technology can or cannot be harnessed in designs
- The software needed to address the desired system functionality continues to grow at a tremendous rate
- With these systems increasingly connected, there are heightened concerns about system security, early detection/mitigation of systems being compromised and abilities to provide updates and/or roll back systems to a known good state
- Much of this functionality is increasingly needed to be implemented near to where the data is created, for reasons that include data privacy, latency, cost and network availability. The industry is increasingly referring to this as Edge Computing

Typically, all of this needs to be accomplished with similar or reduced budgets in shorter development cycles.

Our position is that Edge computing itself is not particularly radical; industries have been oscillating between centralized and distributed computing for decades. What IS different this time is that an increased number of platforms are involved in preserving human life and/or operate alongside humans and many are becoming mobile. The consequences of these systems failing can literally cause lives to be lost or injured.



Source code requirements for new systems continue to grow.

Across markets like aerospace and defense, industrial IoT and automotive, companies are increasingly looking at modular systems that harness open standards. With the extraordinary advancements in powerful-yet-cost-effective semiconductor technology, the functionality that was once implemented in multiple discrete systems can now be collapsed down to run on a single, multicore component. The ability to run rich operating systems like Windows and Linux while providing guaranteeing real-time (measured in microseconds) response to particular events is what Lynx refers to as the Mission Critical Edge.

Lynx estimates that this is an $16B software market opportunity in the 2023 timeframe.

Mission Critical Edge applications include Industrial robots, self-driving vehicles and flight displays.

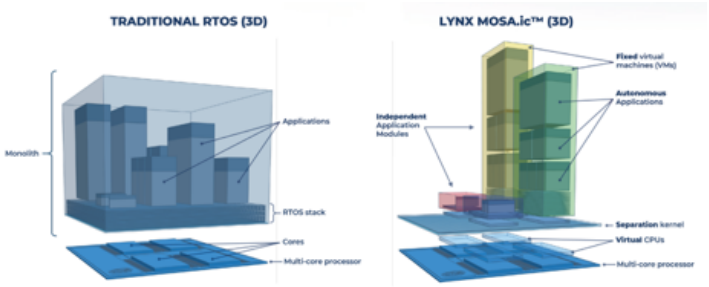
Lynx offers a software framework, called LYNX MOSA.ic, which empowers system architects to combine technology from Lynx, 3rd party operating systems and customer-developed (bare metal) applications in a way where systems are subdivided into smaller, independent stacks which include only the dependencies required.

The LynxSecure separation kernel forms the foundational piece of MOSA.ic, where CPU, memory and IO resources are allocated in a fine-grained way to each virtual machine. There is no "helper" OS in a system that uses MOSA.ic. Key system functions are decentralized and distributed to avoid full reliance on a single operating system. The traceability of hardware allocations on a per VM basis is one of the reasons why it is easier to certify platforms that harness LynxSecure. These configurations are immutable after system boot, and Lynx's patented technology ensures these applications are isolated from each other, which enables system architects to guarantee real-time deterministic behavior no matter what else may be occurring in the system.

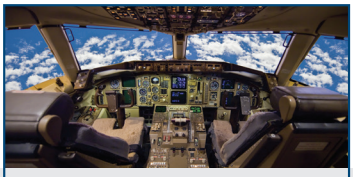
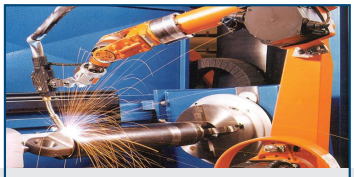
In the middle of 2020, Lynx released a series of products that harness the MOSA.ic framework. Each product features three elements of software;

- Lynx software products; LynxSecure, Luminosity, LynxOS-178
- Guest operating systems; Windows, Linux, Real-time operating systems
- System integrations; Azure IoT Edge, Kepware, Kubernetes etc.

The elements taken from each of these three categories will vary based on the types of applications being addressed. Specific proven combinations of software products that address specific applications are shown in the table below. In the area of avionics, this includes Lynx's LynxOS-178 real-time operating system which brings the benefit of a large amount of certification work, including a reusable software component (RSC) approved by the FAA, and compliance with a number of popular open standards such as Future Airborne Capability Environment (FACE), ARINC 653 Application Executive (APEX) and POSIX. For the industrial market, there is more emphasis of guest operating systems and providing secure, real-time deterministic system to system connectivity, with support for cloud services, containers and data distribution networks.



LYNX MOSA.ic PRODUCT OFFERINGS

	Avionics	Industrial	UAVs & Satellites
			
Example Applications	Cockpit avionics Mission Control	HMI platforms Industrial robotics	Commercial drones LEO Satellites
Supported Integrations	• Implemented with Lynx professional services	• Azure IoTEdgerntime • Virtual PLC • Data analytics • Kepware (legacy interfaces)	• Kubernetes (container) orchestration
Supported Guests	• Linux • LynxOS-178	• Windows 10 • Debian-RT • CentOS • Ubuntu • FreeRTOS • AzureRTOS	• Linux • LynxOS-178
Lynx Componenets	• LynxOS-178 • LynnxSecure • Lynux Simple Applications • Certification evidence • Tools	• LynxSecure • Lynx Simple Applications • Tools • Manageability	• LynxOS-178 • LynnxSecure • Lynux Simple Applications • Tools • Manageability

Joint Strike Fighter (JSF) Technology Refresh 3 (TR3) program

The JSF is the US Department of Defense's focal point for defining affordable next generation strike aircraft weapon systems. A key element of the "Technology Refresh 3" (TR3) modernization program for the F-35 Lightning II avionics platform is the adoption of commercial-off-the-shelf (COTS) technology and an Open System Architecture as an approach to addressing this. The Integrated Core Processor (ICP) in this platform processes data for the aircraft's communications, sensors, electronic warfare, guidance and control, cockpit and helmet displays. The LYNX MOSA.ic framework was adopted as it enables the TR3 subsystems to be cleanly architected from reusable software components that avoid proprietary dependencies. From a business perspective, the adoption of technology from Lynx for the TR3 program enables to development-, sustainment- and acquisition costs to be drastically reduced and provides the necessary flexibility to implement system upgrades well into the future.

Secure Laptops

Some agencies, with tens of thousands of agents, each utilizing up to 5 dissimilar devices daily, have very limited remote access to the Agency's secure internal network. This results in severe productivity constraints, cyber security risks and sky rocketing maintenance costs. Our partner, a federal IT provider, has defined a set of laptop & tablet configurations that meet the Commercial Solutions for Classified Program (CSfC) data assurance requirements and usability expectations for remote access. LynxSecure has been selected for a next generation laptop program due to the unique isolation properties included in the product, coupled with our flexibility to tailor the product to their unique requirements.

Gray Eagle, General Atomics

General Atomics - Aeronautical Systems, Inc. (GE-ASI) from San Diego focusses on the development and production of For the Gray Eagle UAV platform, GA-ASI requires a secure, reliable and repeatable platform to ensure the demanding and exact performance of their UAV. There was also a need to provide a path to meet aviation DO-178C requirements, and isolate multiple security levels. The Lynx solution was felt to provide a foundation for constructing modular systems offering real-time, security, and certifiability and Incorporates purpose-dedicated software enclaves each with operations and access restricted to their precise need. The LynxSecure hypervisor is lightweight and so avoids any performance limitations.

Scalable Safety

Supporting modern avionic software requirements is incredibly costly. Testing alone for DO178C compliance will cost vendors tens of millions of dollars for a modest set of RTOS features to meet Design Assurance Levels (DAL) C or higher. Multicore integrity and timing analysis for airworthiness certification adds additional program costs and technical risk of comparable magnitude. The FAA introduced the concept of the Reusable Software Component (RSC), which is software that can be integrated into many systems' target computers and environments. LynxOS-178 is the only RTOS awarded the FAA RSC, passing forward the safety certification reuse benefits to developers building safety critical software against standard POSIX APIs and a Unix-like File System, fully certified to DO-178C DAL A.

AIRBUS
BAE SYSTEMS
BOEING
BOSCH
Collins Aerospace
GE Aviation
GENERAL DYNAMICS
LOCKHEED MARTIN
L3HARRIS
NASA
NORTHROP GRUMMAN
Sandia National Laboratories
Raytheon
TOKYO ELECTRON
Wabtec CORPORATION

"Lynx's DNA is centered on ensuring the operational safety of the platforms our customers create, certify and deploy. Our foundational software technologies have an essential role to play in an increasingly broader set of markets that value reliability, deterministic real-time behavior and security. I am excited about our strong capabilities that advance Lynx, our partners and our customers!"

Scalable Security

LynxSecure, Lynx's separation kernel, is certified, fielded, and maintained on classified DoD networks. The product has undergone many security assessments, including penetration testing and design review by independent government security authorities. Lynx optionally provides a Risk Management Framework guide to aid the security evaluation of the security enforcing properties of the platform. The package includes NIST security control traceability and Common Criteria Security Target traceability into the underlying kernel design requirements. For customers interested in kernel source code control and deeper levels of traceability and security analysis, source code and low-level traceability is offered as an additional package.

Lynx background

For over thirty years, Lynx Software Technologies has helped customers (some examples below) with some of the most demanding, mission critical, system requirements to create, certify, and deploy equipment, above, on and below the surface of the earth.

It is critical to Lynx that we understand your specific goals, target environments, and unique design challenges. We promise to be transparent and be forthcoming about technical gaps and to only provide recommendations that have been thoroughly verified. We have zero interest in creating added challenges for our customers through dishonest and/or haphazard business practices and will work tirelessly to deliver unparalleled lifetime value at fair and competitive cost.

Milestones in Lynx History

1988	Lynx Incorporated
1998	HP 4550 Printer
1998	Boeing 777 Cabin Management System
2000	BlueCat Linux
2000	Jetstream CPX 1000
2002	LynxOS-178
2002	Royal Danish Navy Standard Flex 300
2003	Skycam CF Inflight
2003	Turbine Diagnostics TurbboNet Dash1
2003	Innovative Concepts Improved Data Modem
2003	Paradise Datacom Satellite Data Modem
2005	Future Combat System
2006	Joint Strike Fighter
2006	Airbus A380
2007	iRobot RGator
2008	Wabtec
2009	ValidEdge Inc.
2010	General Dynamics Integrated Computer System
2011	Elekta
2013	ValidEdge to McAfee
2013	DDG 1000/Zumwalt Common Display System
2014	CISCO Catalyst Family
2016	Bosch/ETAS
2016	Ampyx Power Wind Energy Generation System
2019	Joint Strike Fighter
2020	LYNX MOSA.ic for the mission critical edge
2020	General Atomics Gray Eagle

1.800.255.5969

CERTIFIED ISO 9001:2015 COMPANY

Lynx Software Technologies, Inc.
855 Embedded Way
San Jose, CA 95138-1018
+1 (800) 255-5969
+1 (408) 979-3900
+1 (408) 9793-920 fax
inside@lynx.com
www.lynx.com

Lynx Software Technologies UK
400 Thames Valley Park Drive
Thames Valley Park
Reading, RG6 1PT
United Kingdom
+44 (0) 118 965 3827
+44 (0) 118 965 3840 fax

Lynx Software Technologies France
38 Avenue Pierre Curie
78210 Saint-Cyr-l'École
France
+33 (0) 1 30 85 06 00
+33 (0) 130 85 06 06 fax