LYNX|Secure®

The Foundation of the Lynx MOSA.ic Framework

LYNX MOSA.ic Framework

The LYNX MOSA.ic framework extends the LynxSecure separation kernel hypervisor with independent capabilities that can be combined to address safety and security challenges across a broad range of complex, multi-core safety or security centric systems. The LYNX MOSA.ic framework allows these systems to be realized in a Robust, Rapid, and Reusable fashion across multiple generations of products.

The LYNX MOSA.ic framework supports:

- LynxOS-178 – FAA DO-178B/C DAL A RTOS
- Linux
- Windows™
- 3rd party OS – Security OS, AUTOSAR, Ada, commercial RTOS
- Virtual Device Server
- Full Virtualization Server
- Lynx Simple Application (LSA)
- LSA.store - Bare-Metal Crypto Module
- Advanced Scheduling LSA

LynxSecure

The LynxSecure separation kernel hypervisor serves as the foundation of the LYNX MOSA.ic framework.

The technology was designed to satisfy Real-time high assurance computing requirements in support of the NIST, NSA Common Criteria, and NERC CIP evaluation processes which are used to regulate military and industrial computing environments.

Key markets include:

- Industrial
- Medical
- Aerospace
- Financial Technologies
- Automotive
- Defense
- Cyber Security

Common use cases include: critical systems that will undergo multi-year block upgrades; real-time systems which require performance or flexibility beyond what is available from a RTOS; any connected platform that protects critical functions and data from unauthorized access.

LynxSecure runs directly on the platform to separate hardware resources into virtual machines used to host software including: Traditional general purpose or legacy operating system (e.g. Linux® or Microsoft® Windows®), Fully featured or simple scheduler-like RTOS, or Enhanced bare-metal applications called Lynx Simple Applications. LynxSecure provides immutable hardware-enforced separation between each virtual machine to ensure that each will run independent and free of interference from power-on until power-off.

Lynx Simple Application (LSA)

The Lynx Simple Application (LSA) is an enhanced bare-metal application used to encapsulate critical safety or security functions. Unlike an RTOS, there are no underlying asynchronous software activities to affect the predictability, performance or worst-case execution timing.

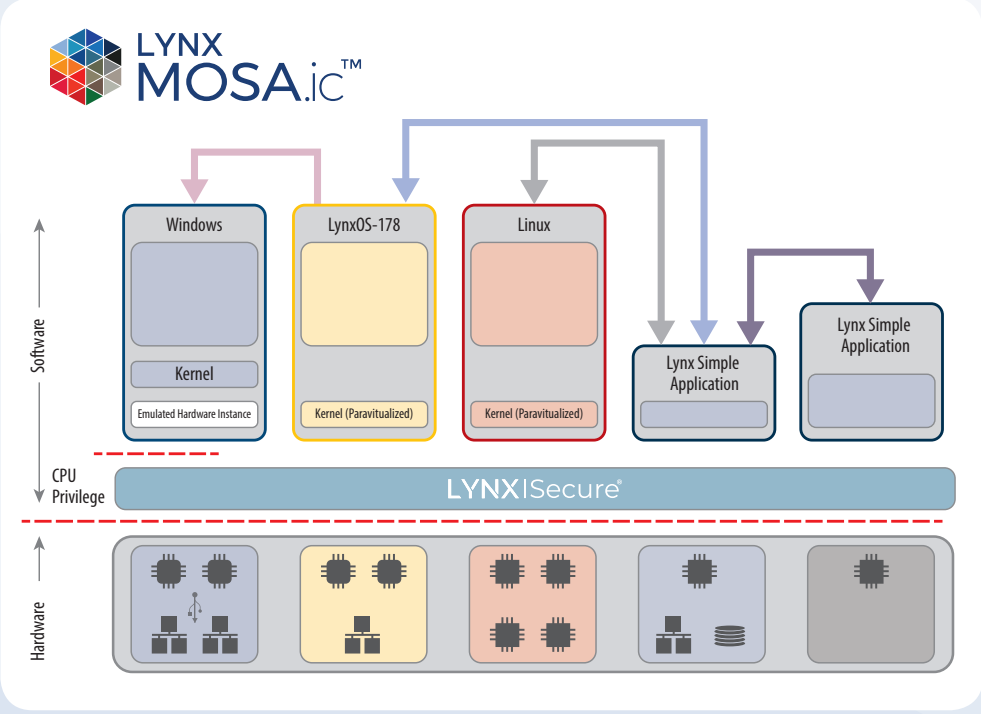

Figure 1: Platform integrity through isolated domains

LSAs can reuse available microcontroller code, or they can be wholly new functions. LSAs can be more easily deployed in future upgrades than the equivalent functionality within an RTOS. Some developers use LSAs side-by-side with Linux or RTOS. Others use them independently, each with dedicated hardware resources; advanced scheduling; and fast, low latency communications.

Advanced Scheduling LSA

A virtual machine can execute on a fully dedicated processor, or on a shared processor using traditional RTOS-like scheduling policies.

Lynx Advanced Scheduling LSA allows developers to build unique scheduling algorithms that ensure the precise and proper execution, timing, and pipelining of critical tasks; even under the most complicated system scenarios.

High Performance OS Interconnects

LSAs provide the ability to dedicate hardware to critical functions without the uncertainties of an underlying multicore OS. Lynx Advanced Scheduling allows the execution of these tasks to be precisely controlled to meet the requirements of complex systems.

High performance OS interconnects provide security-policy enforced, zero copy, fast and low latency communications between critical functions. These interconnects allow any software asset to be securely connected with another asset to efficiently and securely pass data through the processing pipeline.

Platform Assurance with LynxSecure

The LynxSecure separation kernel hypervisor offers advanced resource scheduling, and security controls that exceed traditional operating systems and micro-kernel offerings.

These LynxSecure tunables allow developers to explicitly define how a compute platform executes with traceable evidence — from specification to instantiation, establishing platform integrity for the following design patterns:

- Safety & Security Domain Isolation
- Trusted Execution Environments
- Reference Monitor Plugins
- E.g. Firewalls, IDS, Encryption, Guards

LynxSecure provides a scalable solution supporting deeply embedded systems to high-end workstations and servers for avionics products, weapons systems, and critical infrastructure control systems.

Security Foundation

The LYNX MOSA.ic framework, allows multiple types of operating systems and bare-metal applications to share a single physical hardware platform.

LynxSecure upholds the principles of least privilege featuring limited kernel space functionality, lightweight simple design, and explicit granular authorization of all system control functions. Unlike traditional OS and hypervisor kernels that include drivers, I/O stacks, and application APIs, the LynxSecure separation kernel exports, per the requirements of the developer, all I/O and application support to developer-specified guest(s) running in user space. LynxSecure kernel space functionality is limited to resource partitioning, controlling data flow between partitions, and mediating access to system state change functions. This provides a robust foundation for the development of high assurance, high performance, safety critical and completely secure systems.

Advantages

Better Safety and Security
- Least privilege model — Guests receive only what is necessary
- Immutable configuration — Hardware, security, scheduling
- No underlying RTOS or “Root OS” — Smaller attack surface, less complexity

More Design Freedom
- Distributed architecture
- Advanced scheduling policies
- Zero copy communications

Faster Development
- Modular design
- Traceable from specification to instantiation

LYNX SOFTWARE TECHNOLOGIES

1.800.255.5969

ISO REGISTERED 9001:2008

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