LYNX
SOFTWARE TECHNOLOGIES

Industrial Applications

Unique safety and security software platform for industrial systems

Processing is shifting to the edge

Unlike the digital speakers in your home, these systems need to be fully operational for ten, fifteen or indeed twenty years. There are three big drivers that are causing the decision making on this data to be driven nearer to where this data is being created:

- Privacy—Sending meta data up into the cloud as opposed to data that is traceable back to a specific individual
- Latency—Some are better made locally in real-time as opposed to being sent to the cloud for processing
- Cost—A fraction of the data being sent to the cloud today is being mined effectively for analysis… but it is all being stored which costs the enterprise a significant amount of money

A Holistic Approach to Robust Security

To unlock the full potential of IIoT, trust must be established across a network. That trust begins with platform security; the assurance that computing components are authentic, initialize to a well-known state, and are resilient to unauthorized changes. Once platform security is in place, systems must incorporate network security and monitoring capabilities to ensure system-wide integrity is resilient to unauthorized changes.

Point solutions tend to address symptoms of engineering flaws—e.g patching, updating whitelists, malware signatures, etc. However, reactionary approaches lose effectiveness at scale and fail at catching the first exploit. LYNX MOSA.ic™ gives product suppliers the ability to build in assurance with the knowledge that their device is precisely designed to execute securely in enterprise or control networks without having to rely on layers of firewalls, IDS, and patching systems.

Building a Network of Trust

Adopting any digitization security technology requires careful technical scrutiny to claims of assurance, interoperability with legacy systems, and life cycle maintenance costs. The architecture configuration language of LYNX MOSA.ic allows developers to design in security properties of system devices that must be trusted and need to survive in hostile environments.

Examples of relevant security designs include:

- Boot Security
- Data Protection: Data-In-Transit, Data-At-Rest
- Data and Control Plane Separation
- Separation of Enterprise and Control Networks
- Read-only Monitoring

With LYNX MOSA.ic, evaluators of security properties such as government authorities or safety managers can trace configurations down to processor hardware control, providing formal evidence of robustness and resulting in a holistic approach to system security. Our emphasis for our product roadmap in this area, aligned with the company's vision, is focused on helping companies create robust software stacks for autonomous platforms.

The LYNX MOSA.ic Framework is comprised of three distinct classes of tools
Architecture Design, Module Development, & System Module Integration.

Module development & system module integration

A cross development kit is included for building guests of varying size, quality, and complexity specific to their target environments. Integration tools connect legacy, competitor, or partner-provided guests together.

Architecture design

Virtual Machines Types

- Bare-metal – Raw 64-bit guest contexts
- RTOS – Lightweight context support for real-time scheduling and certified code bases
- Legacy OS – Hardware emulation support for legacy code bases

Lynx CDK guest support

LSA

- Lynx Simple Application (Bare Metal Application)
- LSA.store – Bare-Metal Crypto Module XTS-AES 256
- Z-Scheduling – Real-time scheduling
- Guest IPC – Point-to-Point FIFO
- Debug – Lauterbach TRACE 32 Integration

Buildroot

- Embedded Linux Toolchain
- Guest IPC – Point-to-Point FIFO, Ethernet, UART
- Device Sharing (Intel) – SRIOV, GFX, USB, Storage, Ethernet
- Debug – Eclipse IDE GDB

Types

- FIFO
- Ethernet
- Device Emulation

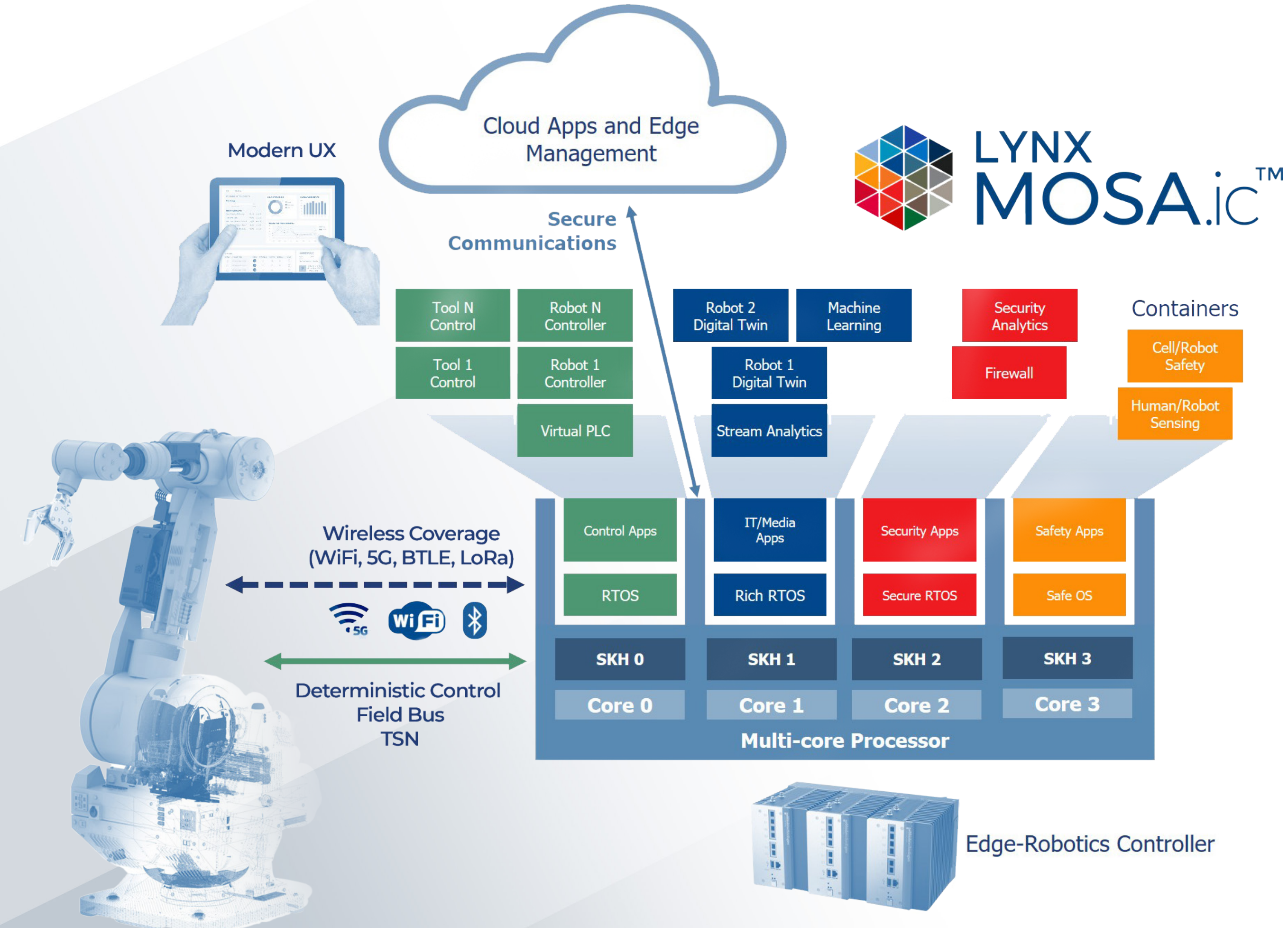
Communication channels—Explicit point-to-point memory regions link VMs together via standard IPC interfaces, maximizing performance and ensuring minimal complexity.

Processor partitioning system

Processor resources are partitiond with an architecture configuration policy to control the behavior of the system. Enforce the policy with a least privilege distributed control plane that creates VMs and communication channels for guests.

Processors

- Arm v8-A
- Intel VTx
- Power PC



LYNX
SOFTWARE TECHNOLOGIES

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