LYNX
SOFTWARE TECHNOLOGIES

Industrial Market Overview

Industrial Internet of Things (IIoT) covers a wide range of applications but a few high-level trends are broadly applicable to many use cases. Firstly, there is a desire to analyze (and subsequently act on the) information nearer to where the data is created than the cloud. The reasons for this include cost, data privacy, latency and desire to not rely on internet availability. Secondly that deployed software and hardware tends to be discrete systems that are several generations off state-of-the-art. Thirdly that the information technology (IT) networks which drive the workflows in a factory are dis-aggregated from the operational technology (OT) networks that are sensing what is happening in real-time.

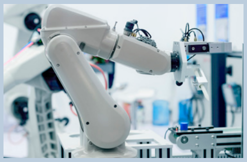
While virtualization is a cornerstone of workload consolidation in the IT networks, OT workflows place larger emphasis on determinism, isolation and safety and security certifications. Its not surprising that the introduction of IIoT paradigms into a typical industrial environment leads to the construction of compute and process islands, mostly emanating from the inability of many virtualization solutions to cater to the needs of virtualization density and scale along with the need for determinism and safety/security.

Lynx describes this convergence of IT and OT paradigms within an IIoT setting as Mission Critical Edge systems. The consolidated systems must solve the following challenges;

- Support legacy hardware and software infrastructure while delivering new edge functionality
- Deliver extremely high levels of system reliability and security
- Achieve deterministic real-time performance

LYNX BENEFITS

For companies creating industrial robots, 5G infrastructure equipment for private networks and industrial automation platforms for green field and brownfield sites, Lynx is able to provide a software architecture that



- Is future proofed for real-time and regular applications
- Offers high system uptime/high immunity to attack
- Provides direct connectivity to cloud services and legacy industrial interfaces, giving the system designer flexibility to select where processing of specific tasks can be implemented based on aspects like CPU availability, price of cloud computation and network reliability

The desire to bring down the cost, power dissipation, and footprint of electronics—coupled with the increased capabilities of modern processors—makes it possible to consolidate functionality that was previously housed in multiple platforms down onto a single processing node featuring powerful multicore processors.

While the technology needs to work as advertised, in order for them to be adopted, the systems need to be shown to deliver significant improvements in business outcomes for specific workflows.

LYNX MOSA.IC FOR INDUSTRIAL

LYNX MOSA.ic for Industrial expands on Lynx's 30-year track record of delivering software to customers creating, certifying and deploying mission critical systems. LYNX MOSA.ic for Industrial blends three elements together, namely;

- Lynx software products; LynxSecure, Lynx Simple Applications and a set of development tools
- Guest operating systems; Windows, Linux, 3rd party operating systems
- System integrations; Azure IoT Edge, Kepware, Kubernetes etc.

Distributed
Data-Analysis Gateway

Multi-Performance
Real-Time Controller

HMI and Visualization

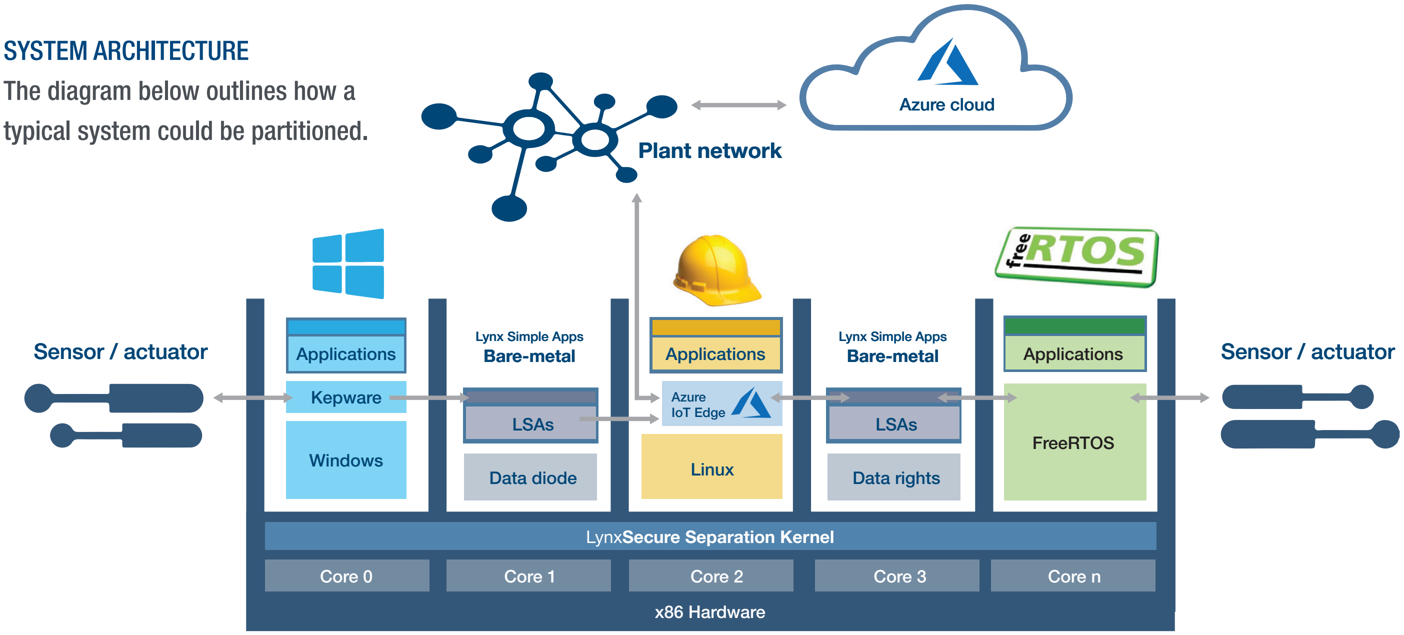
Specialized Parallel
Computing Noodes

Distributed Data
Storage Noodes

The foundational building block is LynxSecure, Lynx's proven separation kernel Type-0 hypervisor. Architects have fine grained control as to how hardware resources such as memory, IO peripherals, and processor cores are allocated to applications. LynxSecure enables mixed criticality systems, with real-time workloads and non-real-time workloads co-existing in an isolated virtualized environment. Buildroot is a simple, efficient, and easy-to-use tool to generate embedded Linux systems through cross-compilation. Lynx Simple Applications (LSAs) are true bare-metal applications, each running directly on hardware without any underlying operating system components. Communications interconnects provide security-policy enforced, zero copy, fast and low latency communications between critical functions hosted on LSAs and guest operating systems. Any LSA or guest OS can be securely connected with any other LSA or guest to efficiently move data through the processing pipeline. Additional operating systems including FreeRTOS and AzureRTOS (both available by end of 2020) will continue to be added, broadening the use cases that this product can solve over time. The series of system integrations enables the Lynx solution to support secure, deterministic system-to-system functionality in addition to providing the desired functionality inside a particular unit. At launch this includes Microsoft Azure IoT Edge, Virtual PLC technology and support of legacy interfaces found in industrial setting via Kepware and Exor's JMobile etc. The alpha release supports Azure IoT Edge running Windows 10 (on LynxSecure) on a Dell platform.

SYSTEM ARCHITECTURE

The diagram below outlines how a typical system could be partitioned.



1.800.255.5969

ISO CERTIFIED 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

©2020 Lynx Software Technologies, Inc.
Lynx Software Technologies and the Lynx Software Technologies logo are trademarks, and LynxOS and BlueCat are registered trademarks of Lynx Software Technologies, Inc.
Linux is a registered trademark of Linus Torvalds.
All other trademarks are the trademarks and registered trademarks of their respective owners.

All rights reserved. Printed in the USA.