

Video Analytics for Industrial Applications

With the widespread availability of high-resolution cameras, coupled with powerful image recognition technology, video analytics is rapidly gaining traction in manufacturing quality use cases. Video analytics is a category of software applications designed to analyze the video stream and draw new actionable insights beneficial to the ongoing operations. They provide a mechanism to automate the identification of people and objects, and a means to trigger a response when things are amiss.

These capabilities make video analytics ideally suited for industrial use cases that include:

- Verification of part transportation and placement
- Quality assurance, parts and final assembly
- Process improvement and proactive plant maintenance

Collectively these use cases are sometimes called visual inspection. These visual inspection solutions are deployed outside the IT domain in factory floors and manufacturing facilities which is also known as the Mission Critical Edge (MCE). The mission critical edge provides the real-time, security and safety of the embedded systems and containerization and focus on data of the edge technologies. Visual inspection deployed at the MCE turn out to be a much more effective solution than the non-AI options which included a human staring at parts coming out of the assembly line or batch sampling it on a frequent basis. These methods were not only ineffective in catching defective parts but also were unable to provide enough data to the production planners to understand the source of the quality issues.

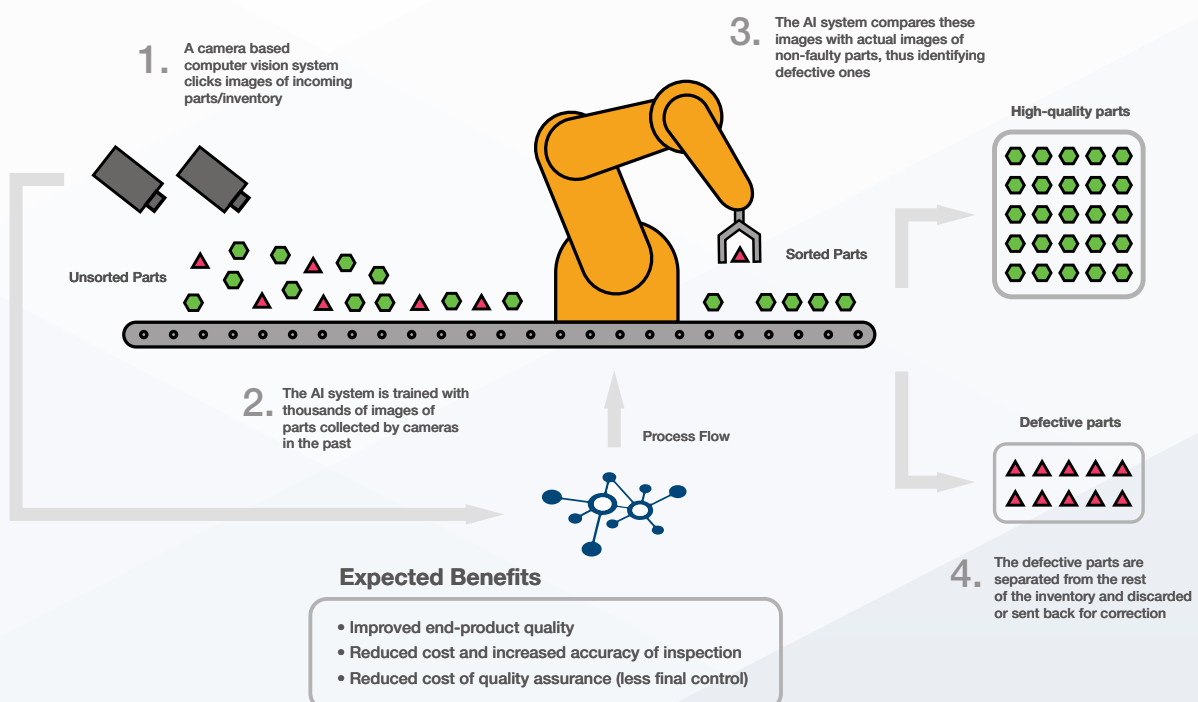
Challenges

Typical industrial video analytics solutions need to handle four key challenges:

- Handling large quantities of data in the form of streamed video or still photographs. This gives them the basis to be able to (say) distinguish a good component from a bad one, or between different part types.
- Integration of multiple, disparate applications, from different vendors, probably using different operating systems. These applications are likely to include Artificial Intelligence/Machine Learning (AI/ML) classification; camera application; picture extraction; production line input and feedback; IoT gateways; and OPC-UA clients.
- Support of multiple network interconnections with dedicated switches and cabling.
- Ability to evolve data models which requires ongoing tuning and updates.

Once these challenges are solved, the video analytics system generates new insights and data that can not only prevent defective parts from going out, but also allow the plant operator to get to the root cause of the defects occurring in the first place.

Computer vision-based quality in action



Delivering on the promise of data

While some companies may have the luxury of a green field environment, the vast majority of companies are faced with delivering this functionality by upgrading existing equipment that is already deployed. Our discussions with companies up and down the value chain associated with delivering connected, secure industrial solutions has led us to view the following as the “best practice” path.

- The majority of existing deployments have a controller connected to an industrial PC type compute node. The initial step is to make these systems managed. By this, Lynx means that it is possible to monitor, deploy security patches and update applications
- Establish a cloud presence. Systems should be able to securely deploy at least one cloud workloads such as machine learning inference engines to the systems and manage those from the cloud
- Ability to run applications from multiple tenants on an Edge compute node, saving power, cost and footprint of electronics. While consolidation is an advantage, the real benefit comes from the ability to leverage video analytics applications that need to procure data from the OT applications, such as a PLC or an industrial camera application, running on the same platform. But for this to be realize, the plant manager needs the confidence that a tenant's applications are able to access only data that they have been granted access to.
- Enable all of the tenants and their different apps to deliver new capabilities that can execute locally while maintaining isolation between the different workloads and preserving data permissions.

Lynx's approach

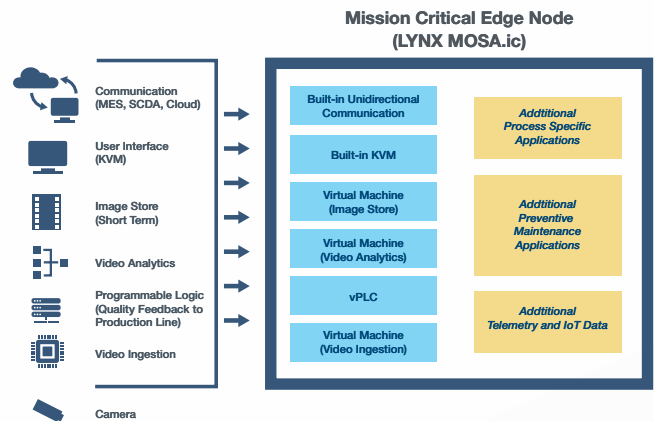
For decades, customer have built solutions on LYNX MOSA.ic that run for 10+ years with very high MTBF (mean time between failure). However, most of these solutions were very largely static with functionality minimized in favor of availability and reliability. But modern solutions that leverage modern AI and container frameworks in addition to running controllers have to be designed to be both flexible and highly available. And to build these solutions that remain viable in deployed settings for very long periods, the solutions need to

- Combine the scaling and upgrade benefits provided by cloud infrastructure with the latency, performance and operational efficiencies delivered by local processing. Lynx refers to this as the Mission Critical Edge (MCE)
- Deliver (provable) isolation between the production line (OT), the plant data center (IT), and the cloud
- Shift as much functionality to software from today's diverse, expensive (in terms of cost, real estate and power) combination of hardware

The following chart outlines how the shift to a software-centric solution enables a wider set of system functions to be delivered over time.

The left side shows all the building blocks needed to build a video analytics solution:

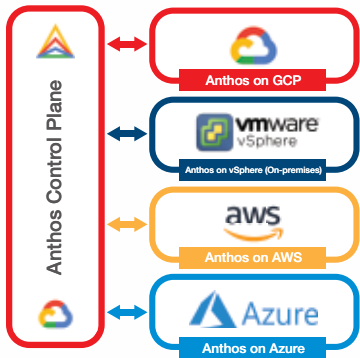
1. Industrial Camera with adequate lighting
2. Video ingestion applications
3. Supervisory control for feedback
4. Video analytics application
5. Image database to store the images
6. IT network access for the video analytics application
7. OT network access for the camera and the supervisory control



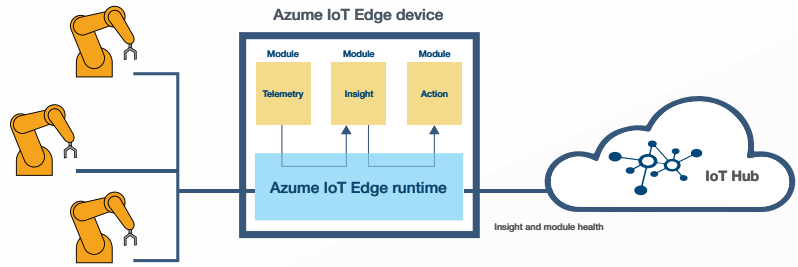
Without LYNX MOSA.ic, a typical implementation would require a separate hardware system for each of these functions making the system complex, difficult to implement and expensive to maintain. But with LYNX MOSA.ic, most or all of these applications can be deployed on a single managed hardware system enabling fast deployment, easy data transfer and seamless management.

Lynx's flagship offering, LYNX MOSA.ic, is a software framework for building and integrating virtually air-gapped security and safety-critical systems using independent application modules. The key capabilities of this offering are:

- **Isolated applications:** It enables fully featured operating systems (e.g. Windows, Linux), real-time operating systems and bare-metal code to be combined and deployed on consolidated hardware platforms in a way that delivers provable (and immutable) isolation of applications from each other.
- **Hardware resources:** It provides for the granular allocation of compute and memory resources to each workload.
- **Peripherals:** The direct assignment of NICs, USB and serial ports enables a complex deployment to be accomplished using a single box. Network connections can be virtualized and secure, providing strong isolation between the operational technologies (OT) and information technology (IT) networks on the plant floor.

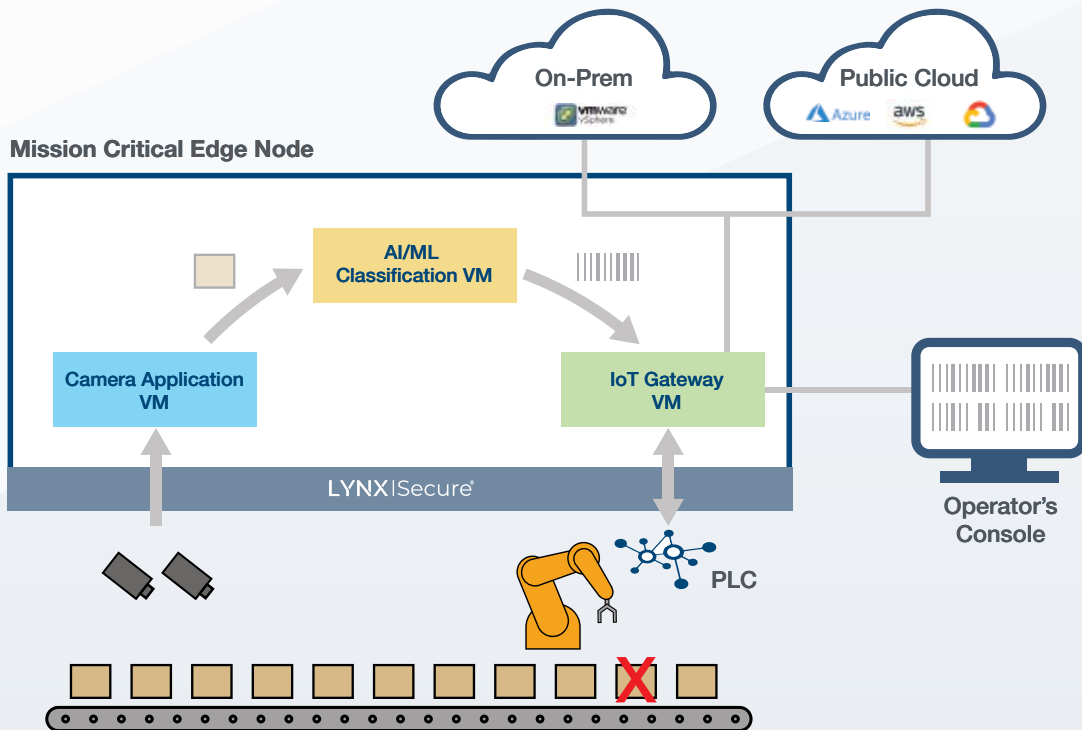


Model 1: Multi-cloud model



Model 2: Cloud extended to IoT

LYNX MOSA.ic is able to provide this level of workload isolation at the HW level since it is constructed using LynxSecure, a separation kernel hypervisor as the foundation. It ensures that the MCE node configuration is tamper-proof and suitable for a harsh production environment, and provides for pervasive security (including data encryption, tamper proof software, and network isolation).



Hybrid requirements

The video analytics solutions at the mission critical edge are required to be hybrid in nature. On the hand, the systems need to be locally managed, handling both OT and IT networks, and the other hand, they have to enable cloud workloads including management of those workloads via cloud portal.

The process specific components – camera, supervisory control, OT network – are typically managed locally. In addition, the management of the system that sets the security and access policies, deploys updates and upgrades is set locally.

The inference model creation using the captured data from the factory floor benefit from the cloud scale and the AI hardware acceleration capabilities in the cloud. Once the inference model is created in the cloud, however, it needs to be run locally on the edge device. The model creation and loading on the edge devices have to be automated such that the model is being constantly updated and refined.

LYNX MOSA.ic allows the line operator to maintain control on the infrastructure while deploying cloud services with the capability to virtually airgap the cloud workloads from the OT network and workloads.

Cloud Models

When implementing mission critical edge solutions that are cloud connected, Lynx is seeing two different approaches being proposed by the Tier 1 Cloud Infrastructure companies. The first of these is to enable multi-cloud environments using technology (e.g. Anthos, an implementation of Kubernetes on Google Cloud) that is supported across a diverse set of Cloud offerings as well as the edge. The second is the extension of the Cloud to the Edge, with a tight, defined communication strategy between the software pieces that operate at both ends of that connection

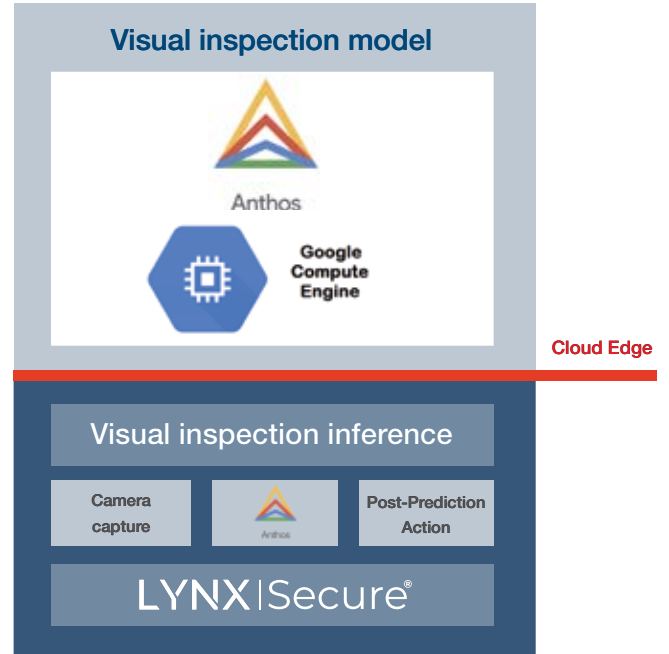
Edge deployment with Lynx

LYNX MOSA.ic can be used with either of these models, but, this document focuses on the approach to enabling multi-cloud solutions, given the strong desire for many customers to avoid supplier lock-in. As shown above, Lynx is using Google's Visual Inspection Service. The model is built on Google Cloud Anthos (bare metal) servers and is run on the Edge node. The edge node can be deployed onto any production line and can now have a combination of local services and cloud services. In this case, the camera capture and post prediction actions are local services whereas the Google Anthos running the visual inspection inference model is locally hosted but managed by the cloud.

The visual inspection use case is just an example of a container-enabled use case deployed at the OT edge. With LYNX MOSA.ic, any containerized services spanning data analytics, security, communication applications can now be deployed at the OT edge.

Summary

LYNX MOSA.ic provides a unique edge capability to deploy hybrid video analytics solution at the edge. Current solutions are either standalone or are managed completely from the cloud. There is a need for a hybrid solution that combines cloud-hosted services for video analytics with local administrative ownership and local process elements such as a camera and a supervisory controller. LYNX MOSA.ic with its ability to provide virtually air-gapped applications gives the plant managers confidence to allow the landing of the cloud services within a carefully carved partition on their OT hardware platforms. In turn, the plant managers can now deploy video analytics, quickly and cost-effectively, towards their desired business outcomes such as quality assurance, parts monitoring and process improvement.



1.800.255.5969



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

©2022 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.