VERACITY
INDUSTRIAL NETWORKS

CASE STUDY: FOOD MANUFACTURING

Challenges with Network Management & Cybersecurity Upgrades

Food manufacturers face a wide variety of challenges when it comes to quality, regulatory, consumer demands, and operations. With the added complexity of cybersecurity, Food companies must prioritize budgets to align with the latest industry standards.

The Background

A large NA Food Manufacturer with multiple facilities scattered across 10 states. The OT network is managed by a 3-person networking team responsible for designing, implementing, and maintaining the industrial communications network. Under constant pressure to deliver safe, high quality food products to consumers, the company must consistently update manufacturing processes and systems.

Challenge #1: Network Downtime

Due to the lack of personnel trained in industrial networking, the manufacturer regularly experienced downtime due to network configuration and changes. The worst incident was a 5-hour shutdown of an entire plant. The issue was a network loopback caused by a maintenance worker who inadvertently moved the wrong cable, which had been reused but never relabeled. Additional issues that continually plague this manufacturer are VLAN misconfigurations and firewall management.

The Solution: Eliminate the Brittleness of Traditional OT Networks

By implementing an OT-SDN (Software Defined Networking) managed network, traditional networking challenges are eliminated. The OT-SDN network controller manages network communications centrally, which removes the possibility of network loopbacks. The solution also brings with it inherent security so VLANs are no longer needed.

Challenge #2: Insufficient Networking Personnel

It is not uncommon for manufacturers to have limited networking expertise in-house. Employees at the plant level make changes to the network at their own risk and the corporate networking resources are stretched thinly across 20+ plants. As a result, incident response takes precedence over new projects.

The Solution: Change the Network Paradigm

An OT-SDN network is presented so that the controls engineer can understand it. A PLC communicates with an HMI in a certain protocol (ex: Profinet or EtherNet/IP). OT engineers can make changes without compromising the network stability or the segmentation. OT-SDN greatly reduces the burden on the corporate network resources, creating time for critical infrastructure upgrades.

Challenge #3: Cybersecurity

With ransomware, DOS attacks, and other security concerns on the rise, the small OT networking team has been tasked with securing legacy and new devices, along with keeping downtime to a minimum. The team created a business case to segment their networks and found that, based on available budget and resources, they could implement 2-3 plants per year. Following this plan, it would take 10+ years to segment the existing facilities.

The Solution: Micro-Segmentation

OT-SDN manages all traffic through an SDN-enabled switch on a device-to-device basis and by communication protocol. Further, OT-SDN can be deployed in hybrid network settings where not all devices are SDN-enabled. A basic network segmentation can be accomplished by converting a distribution switch into an SDN switch, like the Cisco Catalyst 9300. Once converted, the network is segmented simply by how the controller microsegments the communications flowing through the switch. Deeper segmentation can be accomplished with additional OT-SDN enabled switches. OT-SDN increased the velocity of the segmentation projects from 2-3 plants per year to 2-3 plants per month.

Conclusion

The Food Manufacturer benefited from these results:

- **Simplified Network Architecture**: Devices can be easily integrated into an OT-SDN network, and scaling up or down can be achieved through software configuration rather than hardware upgrades.
- **Scalability**: Centralized management of network policies and configurations can be defined and updated dynamically, leading to greater agility and automation.
- **Flexibility:** Network policies can be adjusted dynamically based on changing conditions or business needs, allowing for quick response to evolving requirements.
- **Security:** Granular control over network traffic flows and security policies can be centrally defined and applied dynamically, enabling more effective threat detection and mitigation.

The Veracity OT Network Management Platform is bringing new capabilities to the OT network. Combining OT-SDN with common switching features and the ability to centrally manage all connected devices, OT network control is now a single solution.

To see how OT-SDN would benefit you, visit **veracity.io/product.**

VERACITY
INDUSTRIAL NETWORKS