Whitepaper

The Power of Managed Ethernet Switches in Industrial Environments

Beginning in the early 2000s, many industrial operations began the move to build digital communications and digital backbones into their production platforms. As is well known, there were both proprietary networks and Ethernet-based systems being deployed.

In part, this development was driven by the rapid growth of office-based Ethernet networks and network technology. Manufacturers from a broad range of industries wanted to have the increased level of digital data, sensor information and data from manufacturing devices – such as PLCs and intelligent servo drives – to give better control and management of production systems.

In many cases, these networks were built using unmanaged Ethernet switches – able to handle the network traffic, but without the sophistication managed Ethernet switches offer. Two of the biggest drawbacks of unmanaged industrial Ethernet switches are loss of network visibility and network control, along with increased risk of security breaches from having vulnerable devices on the network.

As the Industry 4.0 revolution proceeds, more and more industrial systems and facilities that were previously isolated, standalone operations are being upgraded with digital sensors and smart devices – and those previously isolated systems are being tied to Ethernet-based networks, ultimately exposing them to the Internet. As industrial Ethernet networks grow in size, the focus on security – on having visibility into what is being connected to the network, if it has the right permissions and if it presents any risk of infiltration of malware – becomes increasingly important.

RISKS OF UNMANAGED ETHERNET SWITCHES

As industrial networks are built out, there has been an increasing drive to connect previously isolated manufacturing systems. This connectivity drive makes sense: many of these manufacturing systems have been generating valuable data, but getting access to that data in real time has required significant investments in industrial networks.

As a result, in some cases, industrial OT organizations have tried to manage costs by using less sophisticated unmanaged Ethernet switches. This approach leaves out the layers of protection and network traffic control that managed switches offer.

Industrial Ethernets are constantly transacting time-sensitive data, in some cases vital input/output (I/O) signals. Responsive I/O and interlock signaling plays a crucial role in preventing equipment failure or damage, wasted product and data loss.

Robust and hardened Industrial Ethernet switches, such as the Red Lion N-Tron® Series NT5000 managed switches, are readily available. Unlike some products on the market, which have been adapted from Ethernet technology used in office networks, these systems have been engineered and manufactured for reliable operation in industrial environments with high levels of vibration and ESD and surge protection.

For a standalone automated production system, such as a bottling machine, the internal network in the machine typically needs to connect the machine's programmable logic controller (PLC), human machine interface (HMI), sensors and other I/O connected devices, a low-cost unmanaged switch connecting the machine's PROFINET or Ethernet I/P backbone was sufficient.

However, those kinds of machines are quickly being replaced by automation networks. Once the network device count goes higher, or a formerly standalone piece of automated equipment is interconnected in a plant with dozens of other systems and intelligent devices on virtual local area networks (VLAN), the need for a managed industrial Ethernet switch quickly becomes apparent.

SECURITY BECOMES PARAMOUNT

Unmanaged switches do not have the software layers managed switches have to exercise real control over how traffic traverses a network and what devices can be attached. With unmanaged switches, it's possible for anyone to plug a PC into the switch and access that network segment, potentially finding pathways into larger parts of a manufacturer's OT or IT platforms.

Managed Ethernet switches can provide what is often referred to as "defense in depth". This concept was incorporated into and formalized in the ISA/IEC 62443 series of standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance.

Following these standards, managed industrial Ethernet switches have multiple overlapping layers and features to provide the maximum amount of protection against a risk factor. If someone wants to add a device or PC to a system with a managed network switch, these overlapping layers can include advanced password encryption capabilities, MAC security, configurable password length and multi-level user access control. Managed Ethernet switches can be easily programmed to automatically disable user or port credentials after a set number of failed access attempts.

Many hacker groups and internet criminals continually target the industrial elements of corporate networks, in part because many still have unmanaged Ethernet switches that provide vulnerable access points they can exploit. With these kinds of features, the industrial network can be equipped with the same password management, control and updating practices established by the IT department for the rest of the company, elevating security and implementing the kind of defense in depth that is vitally necessary for dependable and active cybersecurity.

IMPROVING NETWORK TRAFFIC AND EASING CONFIGURATION

Industrial Ethernet networks are becoming increasingly complex and traffic heavy. To minimize networking delays, and therefore improve the level of determinism on any network, it is important that communication data packets be transmitted from the source to the target device. When packets are transmitted where they are not needed, destination devices expend resources to handle the packet, delaying processing of critical communication.

Managed switches give automation engineers exceptional control over these kinds of issues. For example, in a large machining department with multiple machine tools networked together, each work cell may have multiple devices within each tool – such as variable frequency drives (VFD) – generating high volumes of network traffic.

That VFD data may be useful for preventive maintenance and system performance tracking, but it may not be necessary for that data to also be passed up to the PLC in the work cell. Managed Ethernet switches like the Red Lion NT5000 have sophisticated access control lists that automation engineers can use to define that – for a specific MAC address – the broadcast would never traverse the link that goes to the PLC.

This same feature can also be used to limit what additional devices or network links can be connected to a particular uplink port. That can also help ensure a given work cell or automation network segment has its traffic properly managed.

With managed Ethernet switches, it can be as easy as powering up the switch, adding an IP address and configuring the device to conform to all the password and network security protocols for that part of the network.

It may appear managing these kinds of traffic and network security features can be time-consuming and complex. However, many leading industrial Ethernet managed switches have been designed for fast, easy, virtually "plug-and-play" installation and configuration. For example, the Red Lion NT5000 Gigabit Managed Ethernet Switch features a quick start wizard that walks administrators through switch configuration for fast deployment. It also supports text-based configuration files, making it easy to retrieve the configuration from one device for redistribution to other NT5000 devices being added on the network.

This is especially valuable in industrial environments where integrating managed Ethernet switches is often assigned to controls or automation engineers, whose backgrounds and training aren't necessarily grounded in Ethernet network configuration tasks and processes. With managed Ethernet switches, it can be as easy as powering up the switch, adding an IP address and configuring the device to conform to all the password and network security protocols for that part of the network.

The latest generation of switches come pre-configured, supporting all the necessary protocols – such as IGMP snooping. Many platforms feature simple graphical user interfaces that include a logical view showing active ports, power supply, temperature and contact relay status, along with color-coded gauges for port traffic and event tracking.

This lets administrators quickly identify and address possible network disruptions in real-time, backed up by diagnostic tools that allow for faster analysis and isolation of network issues to help maximize network uptime.

THE VALUE OF INDUSTRIAL DATA

Many manufacturers recognize their most valuable asset is their industrial data. In Industry 4.0, as they implement or upgrade their industrial networks to take full advantage of the speed and power of industrial Ethernet systems, there are clear advantages to investing in managed industrial Ethernet switches.

They give industrial users easier, more secure and more reliable access to all that valuable data, with state-of-the-art features to minimize cybersecurity risks and give plant managers critical visibility and greater control of their industrial networks.

About Red Lion

Red Lion is focused on being THE Industrial Data Company™. We empower industrial organizations around the world to unlock the value of data by developing and manufacturing innovative products and solutions to access, connect and visualize their information. Red Lion's global manufacturing and support facilities serve customers in factory automation, alternative energy, oil and gas, power and utilities, transportation, water and wastewater industry segments. We provide scalable solutions for cloud connectivity, edge intelligence and asset management, industrial Ethernet switches and industryleading panel meters and operator panels, to make it easy for companies to gain real-time data visibility that drives productivity. Red Lion is part of Spectris plc, the experts in providing insight through precision measurement.

www.redlion.net

RED LION®