Industrial Networking 101

Differences between Networks for Industrial Automation and Control Systems and Networks for Enterprise Information Systems

Malisko
ENGINEERING, INC.

Table of Contents

SECTION I
Introduction

In the past, networks for Industrial Automation and Control Systems (IACS) used entirely different hardware and software than networks for enterprise information systems. Once Ethernet and Windows matured in the 1990's, IACS networks began using similar technology as enterprise IT networks, except IACS networks used hardened hardware that could stand up to the sometimes harsh conditions of the industrial plant. While this technological progression helped improve industrial networking, many IT enterprise administrators started treating IACS networks the same way they'd treat enterprise networks in the areas of topology design and equipment sourcing. Due to the differences between industrial and enterprise environments, this often caused disastrous results.

In the following list, we show you the areas where industrial and enterprise networks are different and how they should be treated differently.

Section II
The Differences

Availability

System and device availability is critical in industrial networking. In order of importance, industrial networks are concerned with Availability, Integrity, and Confidentiality (AIC) of data. With enterprise networks, it is Confidentiality, Integrity, and Availability (CIA) of data. But in an IACS, a network outage is a loss of production, which translates to an immediate loss of income. While important in an IT enterprise network, availability is usually not critical for short-term outages.

Topology of Network

IACS networks are often small, consisting of workstations/HMI, controllers, and controller level devices — usually with static configurations. Each network, or cell, is made up of just the devices necessary for a specific process. By comparison, IT networks are often much larger and can have thousands and thousands of nodes and automated tools, such as DHCP.

Segmentation of Network

Because of the requirements and differences between IACS networks and enterprise networks, there must be a boundary between the two networks — a Demilitarized Zone (DMZ). Data such as normal LAN data, email, and Internet access can never be allowed to coincide with data communication and Common Industrial Protocol (CIP) data between controllers and I/O devices. These data interactions can cause delays that can keep an I/O device from properly responding to a controller, leading to production delays and compromised quality.

IT Components

There are environmental differences between enterprise and IACS areas. The outer casing of network components, such as routers, switches, firewalls and workstations, must be hardened for harsh environments that have extreme temperatures and humidity. The enterprise environment where network equipment and servers are kept is typically clean and temperature controlled, unlike the plant area where equipment can often be located close to each manufacturing zone. The software and operating systems are also hardened in industrial networks.

Safety Instrumented Systems (SIS)

It's critical for industrial plants to have distinct but integrated Safety Instrumented Systems (SIS). The SIS is necessary to place processes in a safe state when conditions that threaten safety are detected. The enterprise network has nothing similar to this. These are proprietary systems that are segmented and isolated from the IACS network. This isn't normally within the skill set of IT enterprise administrators. To ensure the SIS' integrity, it often takes manual effort to protect the SIS from the IACS network and other external factors.

Software

Industrial routers and switches come with software operating systems that are designed specifically to work with the operation and diagnostics of the controls network environment. Controls messaging, known as Common Industrial Protocol (CIP), is embedded into industrial switches and routers. CIP is used as the industrial standard to eliminate vendor specific software for configuring and monitoring industrial devices — such as Human Machine Interfaces (HMI), Programmable Logic Controllers (PLC), and other Input/Output (I/O) devices. Having industrial standard CIP and eliminating vendor-specific software allows industrial programming software to display screen panels, or faceplates, that automation and controls professionals use to integrate networked devices. An enterprise network equivalent to CIP is the SNMP protocol, but CIP messaging uses many times more tags, or bits, of information. And unlike SMNP, which is only used for monitoring, CIP is used to control devices.

Patching

Patches for software and hardware are usually deferred or postponed indefinitely on IACS networks. They are often quickly installed on enterprise assets. Patching is required on a regular basis in enterprise environments to ensure security and compatibility with other applications. But many IACS systems are so old that patches are no longer available, with many systems still running Windows XP and NT OS. In an IACS network, an improperly executed patch can knock production offline or even cause major safety concerns for operators.

Security

Most enterprise networks require single-factor authentication, such as login names, passwords and PIN's. But producers need to know who's starting or running processes in the plant, both for safety reasons and for the integrity of a manufactured product. Only a set group of users are allowed access to any given production area or process in a plant. That's why industrial networks are increasingly going a step beyond enterprise networks in security by requiring two-factor authentication. The first factor is a something you know, such as login, password and PIN. The second factor can be something you have or something you are.

An example of something you have is a Radio Frequency Identification Device, or RFID, that could be embedded in a card, wristband, or article of clothing encoded with your identity. Something you are can be biometric, such as your fingerprint or your retina. Fingerprint and retina are unique to each individual and can identify a specific person. It's possible to obtain someone's login and password, but it's harder to obtain their user name, password and RFID, retina or fingerprint. To gain control of a console or panel, you would need to present an RFID device or retina or fingerprint in range of a sensor, then input a password or PIN. These two combined

factors will authenticate you are authorized to control a specific process in a specific plant area.

Section III
Communication is Key

These are some of the differences between industrial and enterprise networks. Not understanding the differences can cause conflicts between enterprise and IACS network administrators. Good communication between the two sides can resolve conflicts.

More about Malisko Engineering

Malisko Engineering, Inc. was founded in 1994 from humble beginnings. We've grown into a multi-disciplined team of engineers, designers, programmers, automation, network, and validation specialists. We deliver cutting-edge automation technology in rapid project time-frames at competitive pricing. We deliver our work on time and on budget. We help our clients meet their goals with well-planned system design and implementation.

Ask a Question

Have a question about this white paper or do you want more output, fewer lost batches and better reports? We can show you how to improve your production and maximize your successes through industrial automation.
Call us at 314.621.2921 or **click here to get in touch**.

Malisko
ENGINEERING, INC.

Regional Office
1009 Grant Street
Suite 200
Denver, CO 80203

Corporate Office
500 N Broadway
Suite 1600
St. Louis, MO 63102

Regional Office
316 N Barstow Street
2nd Floor, Suite A
Eau Claire, WI 54703

malisko.com