CONTROL SYSTEM
CYBER SECURITY

Data Is Stale, But The Process Is Running

SYSTEM FAILURE
error 235553261...pending.....
fatal ER # 5444167QW32Z_WS @4$$

Author: James McGlone, Kenexis

What if a hacker just made it so your operators could not tell if your process was running correctly while the hacker did something bad?

This is a common cyber threat scenario and yet we often see processes running where the operator has learned to ignore stale or missing data. Operators often will get up and take a walk to insure the operation is working correctly and then wait for the data to update.

The weakness you deal with daily is the weakness the hacker will exploit.

While it might be unlikely that an actual hacker would cause this situation at your facility, the result is the same and it's being caused by problems with industrial communications networks.

As consultants, we have seen machines fail because they could not communicate correctly, and witnessed startups stretch out months because the network and communications were not designed correctly. We witnessed a situation where the customer's team thought they were experiencing a cyber attack, but the industrial control system was actually experiencing a firewall configuration error that resembled a port scan attack.

Sometimes the problems come from noise on the network caused by faulty devices or an improperly grounded cable. Occasionally, it is a misconfiguration that allows an industrial controller to broadcast to everything on the network because the network was not segmented correctly.

Frequently the design is inadequate for abnormal conditions. Steady state operations have plenty of bandwidth, but when a major problem occurs and alarms start sounding, the network becomes congested and fails the operators who are trying to put the systems in a safe state.

So how did we get here and how can we improve our situation?
Originally when we started using computers for industrial control, it was to replace electro-mechanical operator panels with something easier to build and change. The connection from the

computer to the controller was serial or a small local network that was proprietary. Today, the communications between the actual device controlling the process and the operator's display can be very abstract. In many cases, the maintenance and engineering staff can tell you where it is coming from, but struggle to tell you what route the data is taking to get to the display or historian. Consequently, it is not much of a surprise when data does not arrive from every point being monitored and that it never gets fixed.

Likewise, as the software applications began to add more value, we started to use additional computers and servers in our industrial control processes. Advances in Ethernet technology led to inexpensive faster networks and, consequently, led us all into using Ethernet technology for our industrial networks. This connectivity is actually providing immense value supporting business objectives like just in time manufacturing, work in progress reporting, and lean manufacturing efforts while bringing the same network security challenges that everyone else is experiencing to the process control network and industrial control systems.

One direction some critical applications are taking is to isolate the process control or industrial control system from the network completely. People have tried this with some success, but the isolation is extremely hard to maintain because of things like mobile memory devices and remote support scenarios for employees and vendors. It is also important to remember that we connected industrial controllers and devices for good reasons. Connected, these machines do more than they ever did standalone and they communicate valuable information throughout the organization so many decisions can be facilitated faster and with greater accuracy.

Today, we have continually improving Ethernet technology available for process and manufacturing disciplines from many different vendors. Programmable switches are a significant improvement over the department store hub we used not so many years ago. New technology is making it possible to isolate traffic from a control stream and route it to where it needs to go without interference. Additionally, there are new inline, high-speed encryption devices with built in firewalls and deep packet inspection to protect a system or a controller from threats while enabling secure routable communications to other systems.

The adoption of technology is continuing to improve control scenarios and complicate the problem. For instance, industrial protocols are traveling over the same network infrastructure as voice communications and file transfer traffic using protocols like HTTP, SNMP, FTP, and DHCP. This facilitates entirely new control and operational possibilities like opening a video camera display window on an operator interface during an alarm condition. Unfortunately, this type of traffic on the network can cause congestion and consequently gaps in data logging or an operator interface screen to loose important operational data.

Implementing the recommended improvements from a well-done industrial network cyber study will net a better security profile and improved network performance.

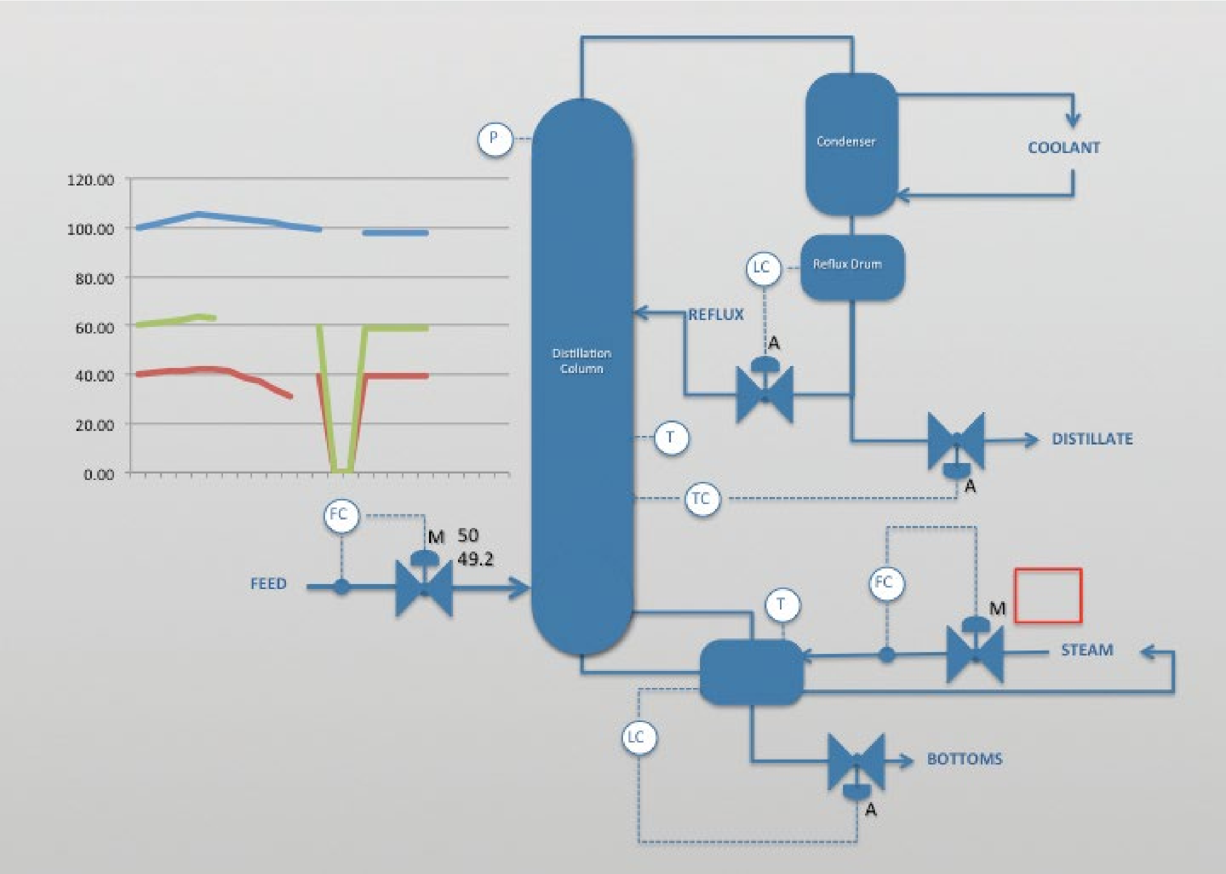
Fortunately, the networks and devices that support the infrastructure consistently improve speed and bandwidth, but our knowledge about the traffic and our ability to know what is actually talking our network is not keeping up. Today, engineers and maintenance personnel, in addition to getting the process up and running and keeping it that way, need to manage redundant industrial application and communication servers, programmable logic controllers, process control systems, safety systems, write code, back up hundreds (sometimes thousands) of configurations and programs. Then they need to maintain version control, patch operating systems and industrial software applications, and upgrade firmware. Now we are also asking them to implement and maintain network systems including switches, routers, firewalls, remote connections, protocols, ports, virtual private networks, network traffic, and network paths just to produce a product. The industrial communications environment is actually much more complicated than the office IT environment.

Many companies have recognized the challenge and are moving individuals into cross-trained roles to function as hybrid IT process personnel. This can be difficult for both engineering and IT since the industrial control environment is not at all like the office environment. IT learns quickly that just running antivirus is harder since you need to check each industrial software vendor's antivirus software exclusion list because scanning the wrong file during operation may cause problems. Even the actual communications are problematic because we use technology like UDP for real-time multicast time-critical communications to many clients simultaneously, and some IT organizations block UDP by default. Additionally, IT learns that the devices on the ICS network are designed to do what they do very well and that they do not like generic IT tools asking them questions. These tools work great in the office, but can stop an industrial control system from communicating or make it go into a fail-safe mode, effectively stopping the machines.

The momentum of technology will continue to fight against getting complete control of this monster. For the same reason we started using computers initially, the problem of abstraction will get worse as solutions begin to utilize virtualization, big data, the Internet of Things, wireless, cloud computing, and whatever comes next. This will continue to challenge maintenance and engineering departments as they struggle to stay current with the technology while focusing on the process and machines.

There will also be tension between lean operating principles and having enough properly trained people with bandwidth to manage your industrial networks. This pressure applied to maintenance and engineering teams will make it hard to apply enough resources to really be good at industrial networking and cyber security. Consequently, other organizations like ours will provide resources to augment your organization focused on industrial network performance and cyber security.

No matter how hard the challenge, cyber security must remain very important to everyone in an organization including operators, engineers, and maintenance personnel. A simple breach through a piece of automation equipment can cause significant damage directly to equipment, alter a process, or maybe just provide access to the company's secret recipe or credit card data. Unfortunately, with or without an actual cyber security attack, your processes may already be experiencing similar problems because of network performance issues.



KENEXIS

GLOBAL EXPERTS IN INDUSTRIAL CONTROL SYSTEM CYBER SECURITY

[CYBER VULNERABILITY ASSESSMENT]

[PENETRATION TESTING]

[NETWORK (DMZ) DESIGN AND
PERFORMANCE ASSESSMENT]

[CORPORATE STANDARDS DEVELOPMENT]