CONTEMPORARY CONTROLS

EtherNet Invulnerability | **Info Sheet**

ABCs of Ethernet Invulnerability

Or how to save your control network from the Gremlins of the office network

Many control networks are connected in some manner to an office network. Many times this is used simply to gather status information from the control network. However, in making this seemingly *innocent* connection from the control network to the office network, many problems can be introduced into the control network. Even without the connection between the office and control networks, your control system may also contain some standard office equipment such as Windows® PCs which can cause similar issues.

The office network can have many network issues which the IT department may not even notice. These problems can be constant or they can come and go as they please. If it takes one or two seconds longer to print a file would you notice? If your webpage took an additional 2 seconds to load would you phone your IT department and yell at them? Probably not. However, your PLC may complain if it takes a few seconds longer to communicate with a motor controller. These types of problems could be catastrophic to your control system.

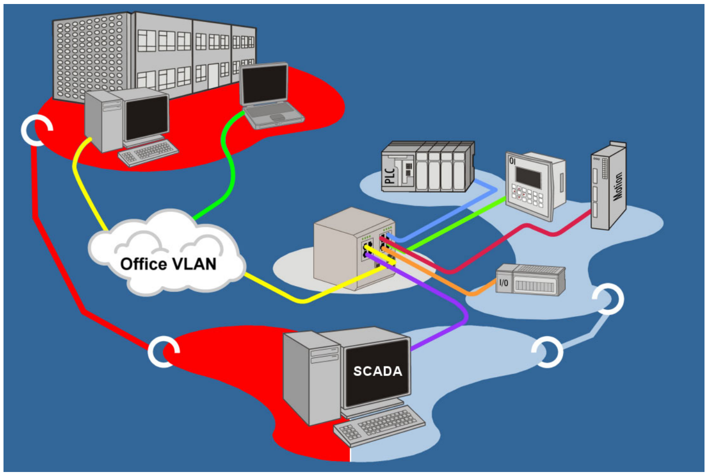
The office network problems can exist as broadcast storms, denial of service attacks, directed message storms, etc. These problems can occur due to such things as improperly wired office networks, incorrect RSTP settings, worms, Trojans, viruses, and Windows problems. It is important to limit the control system susceptibility to these problems. This is especially true if the control engineer has full authority over the control network but almost no control over what happens on the office network.

If you are using office-grade equipment such as Windows PCs in your control network, then you are vulnerable to issues created by these machines.

There are a few techniques which can help protect the control network from these problems.

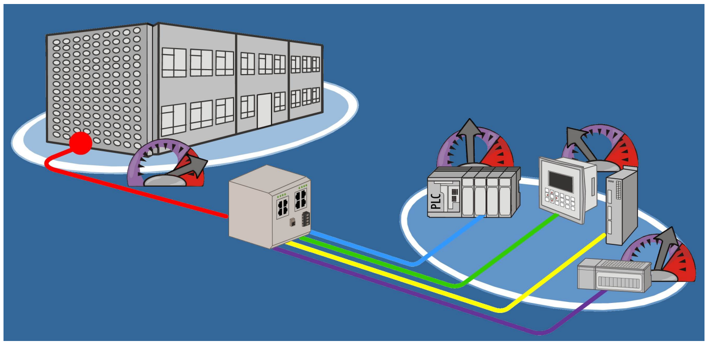
1.) Overlapped VLANs

A VLAN allows for the logical separation of traffic on the network. Devices on one VLAN cannot communicate to devices in another VLAN. However, if you want one device to have access to two or more VLANs then a router or an overlapped VLAN would be needed to provide this type of access. An overlapped VLAN is a special type of VLAN provided by managed switches that can allow one or multiple devices to have access to more than one VLAN. That is, one or several devices can exist in multiple VLANs. All other communications between the VLANs is blocked. Such an arrangement, for example, can allow a SCADA system to be shared between the office network VLAN and the control network VLAN, while blocking all other access between these VLANs. This enables SCADA communication with control network devices and allows office network devices to determine the control network status while protecting the rest of the control network from office network problems. Any office network issues will only affect the SCADA system. The rest of the control system will remain protected.



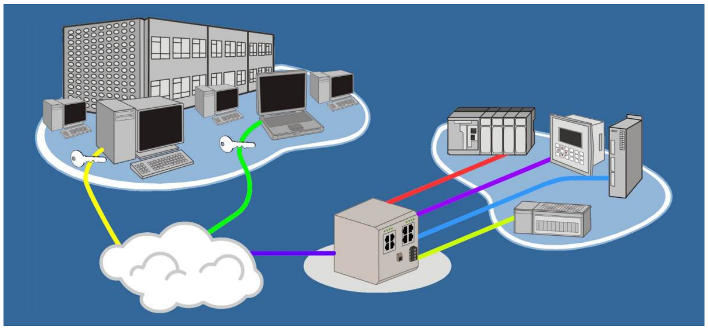
2.) Rate Limiting

Rate limiting is a managed-switch feature which can be used to limit the bandwidth consumed by devices connected to specific ports of the switch. The user can specify a maximum bandwidth for each port of the switch. This can, for example, be used to limit the level of traffic being sent to a sensitive piece of equipment. If your PLC cannot properly control your factory while it is receiving a high level of Ethernet traffic, then it would be advisable to use rate limiting to set the maximum bandwidth to a level that would allow the proper functioning of this device. If your HMI reboots or has other issues when receiving a large amount of traffic, then you should use rate limiting here as well. Another use of this feature is to limit the traffic being sent to the control network from the office network. In this way excessive traffic problems created by the office network, such as broadcast storms or directed message storms can be controlled with rate limiting. If you use Windows PCs in your control system, these devices can cause problems for the rest of the control system. It is recommended that rate limiting be used on all switch ports that connect to any Windows PCs. Rate limiting can also control the level of multicast messages.



3.) Port Locking or Port Security

This feature can be used to control which devices can communicate through specific ports of a managed switch. This can determine which office network devices can communicate with the control network, minimizing the problems presented by the office network. In the example below, all traffic from the office network is blocked except for messages from the computer of the production manager and from that of the engineering manager — each of whom has “an access key”.



Summary

These three techniques — overlapped VLANs, rate limiting and port security — can help safeguard your control network from issues presented by the office network or office equipment such as Windows PCs.

All of these helpful features are available on the Contemporary Controls *CTRLink* line of managed switches (EICP, EISX, and EISB).