Executive Summary
Cyber security means the confidentiality, integrity, and availability of computers, applications, and digital-based assets. In most organizations, this is the responsibility of the corporate IT group. Unfortunately, when IT is involved in real-time control systems, it has lead to political struggling, and misunderstanding of operation’s requirements. If IT implements different Microsoft® Windows® domains and firewalls between plant and business networks, the first casualty is typically DCOM communication, and consequently OPC traffic. Industrial cyber security is complex, and with a skilled assessment and innovative solutions you can ensure your plant assets are protected. Industrial Cyber Security is Powered by Matrikon, which represents vendor neutrality. This product works with third-party control systems and applications.

It is an accepted fact today that Windows is the most popular desktop operating system in the world today, in homes, businesses, and industrial facilities. Thus, Windows has become a popular target of malicious network attacks, which is echoed in the fact that two or more new worms and viruses per month are crippling computers and networks around the world. These malicious applications are so contagious that the introduction of an infected laptop to an otherwise clean network can bring an enterprise down to its knees in minutes. Causing a variety of issues including rebooting computers, corrupting applications, and denial of services to valid users.

The early generation of viruses were the type that infected files, boot records and computer memory. In order for a virus of this type to propagate, it was typically saved to a floppy disk and opened on another computer. File sharing has evolved from physical floppy disks to electronic networks that can reach thousands of computers with incredible transfer rates. Consequently, viruses began leveraging data networks with the intelligence to propagate quickly across a network, earning the new title of a ‘worm’. One of the earlier and most significant worms is CodeRed. It possessed the capability to infect vulnerable Microsoft IIS web servers, then search out and destroy other web servers on the network. In 2001, CodeRed had spread to every vulnerable web server on the planet in 14 hours. Current worms are spreading faster, it is taking less time to propagate and the effects are growing worse (refer to the Brief History of Viruses).

It is for this reason that IT departments are concerned with Cyber Security, and they have good reason to be! Their objective is to protect the users, and all company assets for cyber attack. Unfortunately, IT departments are prone to misunderstand the operational needs of the production side of the business resulting in communication and compatibility issues. One of the first casualties is DCOM (Distributed Component Object Model).

DCOM was developed to provide an easy-to-use communication infrastructure for enabling remote Windows applications and computers to work together. DCOM permits developers to reuse Microsoft’s methods and procedures in their own applications. This accelerates application development and increases reliability. It is for this reason that the OPC Foundation selected DCOM as the basic building block for OPC communication.
# Table of Contents

- Executive Summary ................................................................. 1
# Table of Figures

**Figure 1**: Basic OPC Communication .......................................................................................................................... 4

**Figure 2**: OPC Tunneling Technology .......................................................................................................................... 5
DCOM comes from the IT side of the world. It is easy for programmers to use, but this ease comes at a price. DCOM requires many ports for finding other hosts, resolving names, requesting services, authentication, sending data, and more. If these ports aren’t available, DCOM will automatically search for others. Any port and service used by DCOM is a target to cyber attacks (viruses and worms). So when DCOM security is compromised, all applications are affected including OPC services. The recent Blaster and Sasser viruses attacked the same components that OPC relies upon. Anyone using OPC may be vulnerable to both of these viruses, and more in the future!

As a first step to gaining awareness about new threats, it is suggested that everyone opt-in to security alert email newsletters and pay special attention to any alerts that reference DCOM, LSASS, RPC, Windows file and print sharing, and remote code execution. These components are built upon the same services that OPC relies on; remain diligent, as your systems may be vulnerable too.

Cyber security must be a priority for process control networks to ensure they are not interfered with. It requires more skill and diligence if your organization intends to integrate plant and business systems. Again, due to the pervasive nature of Windows and DCOM, when it is necessary to lock down communication, many applications including OPC are immediately and sometimes terminally affected. Actual events shared by companies include loss of data, visibility, and the even ability to control OPC servers.

Network and cyber security must be a priority, therefore making firewalls a necessity. Firewalls impose many new challenges for DCOM communication. Because DCOM requires a wide range of communication ports to operate, it is very unfriendly to firewalls. Consequently, DCOM is either not allowed communication across different networks or left wide open for worm infection.

Fortunately, if plant and business systems have the right technology, are configured and maintained correctly, network security and OPC can coexist nicely. Innovative solutions are already available for helping to address security for integrated systems. For instance, OPC can make use of tunneling technology working across different systems and firewalls. Similar in concept to a VPN (Virtual Private Network) and PPTP (Point-to-Point Tunneling Protocol), OPC tunneling encloses the data payload inside another protocol. From the outside the tunnel looks like a stream of data. However, inside this stream is the all-important production data. Tunneling technology can also make use of port restriction, user authentication, and data-stream encryption to overcome most of IT’s security issues.

Consider it the use of OPC without the headaches of DCOM. DCOM is still used, but the communication protocol changes to a firewall-friendly and secure alternative. This modular design allows existing OPC installations to remain operational but without the large number of ports open through your firewall.
Tunnelling can also address authentication between different networks and Windows domains. DCOM is a Windows component, tightly integrated with its security features. Traditionally, it was not an easy task to get communication between OPC components on two different Windows domains without a trust between them. The trust allows resources such as files, printers and data to be shared between two different security zones. A trust between plant and business domains is a bad idea and can lead to the propagation of viruses. Tunnelling can replace the DCOM authentication requirements and allow data to flow between plant and business networks seamlessly and securely.

Tunnelling can also ensure the data is protected as it traverses the network, DCOM and OPC do not encrypt information. This could allow a skilled computer user to capture the stream to manipulate or gather sensitive information. Consider the impact of falsified information going to the operator console, or into the control system. The operator may take action on false information, or the control system may carry out a dangerous request. There is also the impact of live production information falling into the hands of the wrong person. To reduce some fears, this kind of event would only work in special situations by skilled individuals. Steps can be taken to mitigate this type of risk.

Effectively addressing cyber security between plant production and business systems is complex. Most information technology and automation groups are hesitant to undertake the task of ensuring control system security. IT may not be familiar with industrial systems, they are complex, and any error can affect production. From the perspective of industrial automation, they can be challenged with IT security and would rather just run autonomously with let a communication ‘gap’ remain between these systems.

In my experience performing security assessments for industrial customers, we have seen many serious problems that staff did not realize were risks. My leading list of issues includes:

- Plant Systems on Business Network
- Bridged/Dual-Homed Servers
- Misconfigured Routers & Firewalls
- Ineffective Backup & Restoration
- Unused Security Features
- Limited Monitoring Capabilities
- Poor Employee/Contractor Awareness
- Lack of Incident Planning
A full security vulnerability assessment (SVA) will identify if these risks and others exist at your site. Every organization should perform and SVA, otherwise they will not be aware of these risks and cannot mitigate them. To perform an SVA it requires the involvement of IT, Automation, Management, Vendors and other 3rd-parties in a combined security effort. Following a defined process, they could identify the vulnerabilities in current OPC deployments and recommend solutions for mitigating them. The most important point to remember when performing a control system security assessment is that existing corporate security policies and procedures may not be feasible and new ones may subsequently develop.

Once again, industrial cyber security is very important to ensure threats do not affect your manufacturing & control systems. Every organization should be completed or about to perform an assessment to identify the potential risks and threats so they can be mitigated as soon as possible. Innovative solutions to help address security risks include OPC tunneling but others will be used to mitigate risks for each threat identified. Get IT and Automation teams together, and if necessary get guidance from a consultant to ensure your production continues.