MatrikonOPC

Effective OPC Security for Control Systems - Solutions you can bank on

Darek Kominek
Manager, OPC Marketing, MatrikonOPC

Eric Byres, P. Eng., ISA Fellow
CTO, Byres Security Inc.

Executive Summary

"There is a perception that control systems are not "popular targets" for attacks. That perception is wrong. Any system made in large quantities is popular enough. If you are involved in any aspect of control systems – especially safety related, you better make cyber security an important part of your processes now. The consequences of ignoring security considerations in some applications can be catastrophic."

Bob Mick, V.P. Emerging Technology, ARC Advisory Group

For the past decade, industrial control systems administrators and engineers wanted to believe that 'air gaps' truly existed between their systems and the rest of the world. They have also hoped that 'security by obscurity' would keep them safe from security threats. Those days are over - recent security incidents such as the Stuxnet worm that attacked Siemens WinCC and PCS7 systems in Iran and the remote sabotage of a Texas power utility are a wakeup call for the industrial automation industry. These aggressive and targeted attacks shed light on just how vulnerable and exposed automation systems really are. They also give us a glimpse of the future of the threats to industry. Ultimately they provide a clear warning: secure your control and automation systems or the reliability and safety of your entire operation is at risk.

While the consequences of cyber attacks and malware are no longer in doubt, the question remains, "Exactly how can an engineer reliably secure his or her control system"? This white paper outlines a simple and cost effective answer – a security solution based on OPC technology that can be deployed in almost any industrial facility today.

Systems are Changing

Information networks have become the heart of the supervisory control and data acquisition (SCADA) systems companies use to provide centralized management and monitoring capabilities. Traditionally companies constructed distributed control systems (DCS) and SCADA systems that were separated from other corporate systems. Such systems were effectively "walled off" by proprietary equipment or protocols.

Business drivers have led to the convergence of company networks and industrial technologies. For example, the demand for remote access for either data access or support has rendered many control systems accessible through non-SCADA networks. Similarly, many companies are reducing network deployment and management costs through shared hardware, backbones and network support resources. Most important of all, the increased use of commercial-off-the-shelf computer components and office-network technologies has transformed the way business is conducted in almost every major industry. These standardization strategies are enabling companies to operate cost effectively, communicate more efficiently and implement more agile business practices through instant access to data throughout the organization, including the plant floor.

While companies reap the benefits of these initiatives, many are also discovering the inherent dangers that result from making control networks more accessible to a wider range of users. Linking corporate systems together to provide access to customers, suppliers, and other third parties significantly increases the vulnerability of sensitive and proprietary information contained in these systems. It also exposes the systems to external events such as worms, viruses and hackers. This increases the demands on system administrators to balance the need for accessibility with the need to safeguard the integrity and usability of their mission critical control systems.

Reducing the Attack Surface

One of the most effective ways to manage the conflict between the demands of efficient access and the demands of effective security is to minimize the variety of interfaces and protocols operating between the control system and the external networks. Having one approved connection solution that serves multiple corporate requirements not only reduces deployment and administration costs, but also reduces the opportunities open to the attacker or worm. This is known as reducing the "attack surface" of a system.

Thus the first task for an administrator is to select an appropriate communications technology that can be used by the widest variety of control AND business systems. While there are a number of possible candidates, including Modbus TCP or Hyper Text Transfer Protocol (HTTP), OPC is without question one of the easiest and most widespread standards to address the demands of universal data access in the industrial automation world.

Example:
Recent significant industrial security incidents #1

The Stuxnet worm, malware designed specifically to attack Siemens WinCC, PCS7 and S7 PLC projects, enters a control system through infected USB keys (so Internet connectivity was a not a requirement for infection). However once inside it spreads to other computers using protocols for file sharing, printer sharing and SQL database access.

Since there were no patches for these "attacks" when the worm was first discovered, the best defense was to not let those protocols reach critical servers unless absolutely needed. Unfortunately, as noted earlier, old fashioned OPC solutions would do just the opposite – every protocol possible was free to be sent to the OPC server, whether it was needed for control or not.

Once known as OLE for Process Control and now officially referred to as OPC Classic , it is the world's most widely used industrial integration standard. It is employed by a broad range of industrial and business applications ranging from interfacing human machine interface (HMI) workstations, safety instrumented systems (SIS) and DCSs on the plant floor, to enterprise databases, enterprise resource planning (ERP) systems and other business-oriented software in the corporate world.

But what about the security demands - can OPC address these? As this paper will illustrate, the answer is a definite YES. By layering defenses that are OPC- aware, high security solutions can be created that meet both the security and access expectations of a company, all without administrative overload on the network or controls team. The result is a standards-based solution that has been proven across numerous different control systems.

Layering Defenses

If reducing the attack surface is the first key to good security, the second is the layering of security defenses. Often referred to as 'defense in depth', the concept is to manage risk with diverse defensive strategies. Layering defenses gives several benefits. The most obvious is that if one layer of defense is compromised, another layer of defense, using a different security method, presents an additional obstacle which can inhibit further penetration.

A more subtle, but equally powerful benefit is that attacks come in different flavors and each defensive layer can be optimized to deal with a specific range of threats. For example, defending against a standard computer worm needs different techniques compared to defending against a disgruntled employee. Thus a key to enhancing each defense in depth layer is ensuring that each layer of security considers the context of the information or system it is protecting.

Defense in Depth: Bank Example

Security in a bank presents a good analogy for the defense in depth approach to security for control systems. What is it that makes a typical bank more secure than a home or convenience store? The bank employs multiple security measures to maximize the safety and security of its employees, customers and their valuables. Not only are there more layers, each layer is designed to address a specific type of threat at the point where it is employed. For example, just to name a few defenses, a typical bank has steel doors, bulletproof windows, security guards, security box keys, safes and security-trained tellers. Bank doors are effective, but simple security devices. They are either locked or unlocked. They either grant or deny access to customers on an all-or-nothing basis – regardless of what a visitor looks like or how the visitor behaves.

One layer up is the security guards – they perform access control to 'clean' the general flow of people into the bank. They ensure that access to the bank is for people who have a legitimate need to be there and will

Example:
Recent significant industrial security incidents #2

In a less famous incident, a major energy complex was infected by a virus in 2009, when a contractor remotely connected to a vibration monitoring system to provide maintenance support. The virus was able to propagate from the monitoring system computers to various DCS servers, causing repeated crashes of key servers and loss of production.

At the time, the site used traditional IT firewalls to isolate the various control systems. Unfortunately OPC Classic's use of dynamic ports resulted in firewalls rules being deployed that were ineffective in stopping the virus. OPC-aware firewalls like the Tofino OPC Enforcer allow much tighter rules and would have prevented the worm from spreading.

'behave' within expected norms. They regard each visitor based on specific criteria, such as, not wearing a mask, suspicious behavior, acting erratically etc.

At yet another level, the tellers, security box keys, passwords, etc. keep these pre-screened customers from accessing other accounts or information. Rather than worrying if a visitor should or should not be in the bank, the tellers and passwords present a different layer of security: account security. These measures 'filter' what account access individual customers are allowed, based on who they are.

Note that the security layers are context specific, which is why banks don't simply have additional security guards at every level. The security solution must fit the context of the threat expected at that level.

Backround:

The term "OPC Classic" refers to all OPC standards prior to the new OPC-Unified Architecture (OPC-UA) standard. This includes the most popular specifications such as OPC Data Access (OPC DA), OPC Alarms and Events (OPC A&E) and OPC Historical Data Access (OPC HDA). Visit the **OPC Foundation website** for more information.

Industrial Control System Security

So what does this have to do with security on the plant floor? Well, for industrial communications the roles of the 'bank guard' and the 'teller' are broadly analogous to 'Network Security' and 'Application-Focused Security'.

For example, the firewall acts like the guard, so that specified protocols are either permitted or denied access into the control network. And just like a more experienced bank guard, a more sophisticated SCADA-aware firewall observes the traffic beyond the obvious protocol types and makes additional filtering decisions based on the behavior and context of the systems using these protocols on the network.

Similarly, an OPC server with a robust OPC security implementation can act like a well-trained bank teller. After a user successfully connects to an OPC server, the OPC Security configuration ensures they only get access to the specific sets of data they are supposed to see. Attempts to access others' data should be blocked and logged.

As with the guard and the bank teller example, the firewall providing the network security and the OPC server providing the application security are an essential team. For example, a firewall can block millions of randomly malformed messages directed at a server as part of a Denial of Service (DoS) attack. At the same time, user authentication and authorization checks can prevent an attacker inside the firewall from accessing process set points in a system and making changes that might risk property or lives.

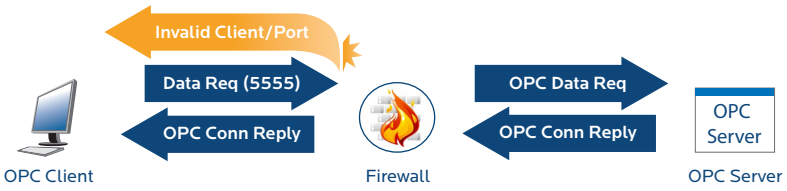
Step 1

The OPC Firewall intercepts a connection request from the OPC client and confirms it is an approved server from an approved client and the message is a properly formed OPC connection request.

Step 2

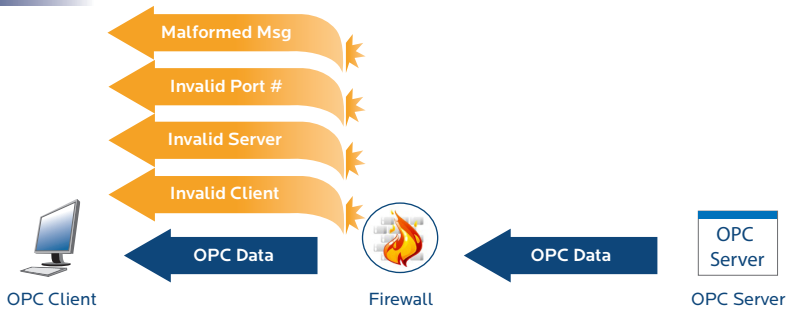
The OPC firewall intercepts the connection reply from the OPC server and confirms it is to original client and is properly formed. It also determines the new TCP port that the server wants to use.

Step 3



The OPC firewall momentarily opens the TCP port it found in the reply message, but only for communications between that client and server. If a proper TCP session does not occurs within a few seconds, the port is closed again.

Step 4



Valid OPC data continues to flow, while malformed messages, messages using invalid ports, or messages from invalid clients or server are blocked and logged by the firewall.

Figure 1 – How OPC-aware firewalls work

Network-Focused Security

To understand network-focused security, it is important to know that most TCP/IP protocols, such as Modbus TCP, include an internationally recognized number (called a port number) in each message to identify the message as being part of a specific upper layer protocol. This consistent protocol identification makes it easy for firewalls to block specific protocol messages or to allow them to pass. For example, to block all Modbus TCP traffic, all a firewall needs to do is search for and then block any message that contains the number assigned to Modbus TCP (namely 502) in certain fields.

An out-of-the-box OPC server does not use a fixed TCP port number. Instead the server dynamically assigns a new TCP port number to each process that it uses to communicate with OPC clients. The OPC clients must then discover these associated port numbers by connecting to the OPC server and asking what TCP port number they should use for the session. OPC Clients then make a new TCP connection to the OPC server using the new port number. OPC servers may use any port numbered between 1024 and 65535 which makes OPC Classic "firewall unfriendly".

On one hand, configuring a traditional IT firewall to leave such a wide range of ports open is like having a sleeping bank security guard watch the front door. On the other hand, insisting on locking down these ports effectively ends up blocking OPC communications. Today, the OPC dynamic port allocation issues are no longer an excuse not to install firewalls in front of OPC servers. New OPC-aware firewalls can now automatically track and manage OPC Classic's dynamic port problem. These firewalls are designed to be dropped into existing networks without any changes to existing OPC clients and servers.

A good example is the Byres Security's Tofino Security Appliance with the Tofino OPC Enforcer™ - a security appliance and OPC firewall. Such devices are designed to be installed in a live control network with no network changes and no plant downtime. They are a simple and cost-effective way to create zones of security in a control system, as recommended by ANSI/ISA99, NERC CIP and IEC Standards.

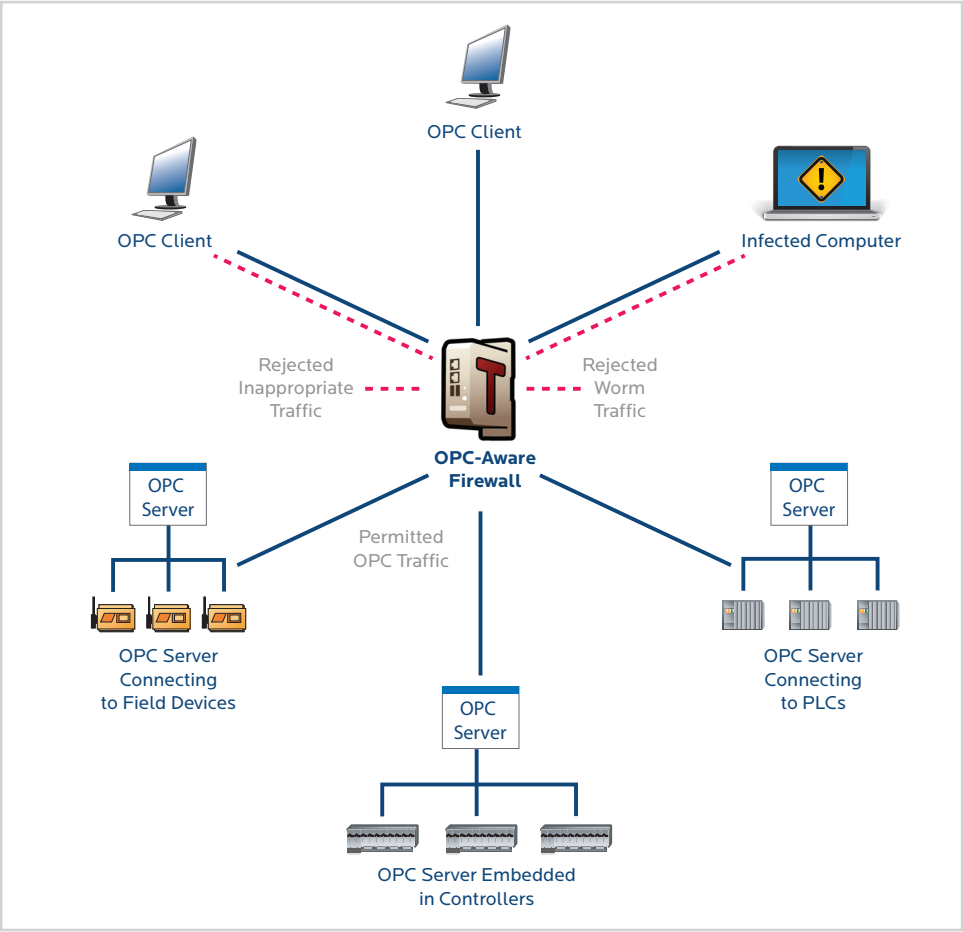


Figure 2 – An OPC-aware firewall safeguarding OPC clients and servers

Application-Focused Security

Returning to the bank analogy, once visitors get past the front door and the guard they approach a teller to take care of their transactions. The teller's job is to both facilitate transactions and to ensure only those accounts the visitor has access to are affected. The OPC servers of virtually all OPC vendors simply rely on DCOM to address security (the guard at the door) and do not provide specific access control security (the tellers).

Access control security, or application-focused security, must be addressed through OPC-specific security measures and through properly designed OPC architectures. As connectivity continues to expand throughout the enterprise, properly implemented defense-in-depth is crucial. Without it, systems exposed to a growing list of threats may not work within target parameters, potentially causing expensive safety, environmental and production incidents.

While many OPC installations rely on corporate firewalls and proper DCOM configuration for security, assessments show that open firewalls and permissive DCOM access rights remain common vulnerabilities. Even in cases where systems are configured correctly, they still do not offer the granularity of security needed to fully protect the system. What is the problem? Corporate firewalls and general Windows DCOM security are not aware of the OPC context. Only by using security products that are OPC 'aware', that support the OPC Security specification, and that properly utilize the information this provides is it possible to provide an effective level of protection.

OPC Server Security Options

Any OPC server or product has the option to implement one of three levels of security: Disabled, DCOM or OPC Security. Each level offers more security and control over who has access to data within the OPC architecture.

- Disabled Security – No security is enforced. Launch and Access permissions to the OPC server are given to everyone, and Access permissions for clients are set for everyone. The OPC server does not control access to any vendor specific security functions.

- DCOM Security – Only Windows DCOM security is enforced. Launch and Access permissions to the OPC server are limited to selected clients, as are the Access permissions for client applications. How ever, the OPC server does not control access to more specific security functions. This is the default security level provided by DCOM.

- OPC Security – Supports the OPC Security specification. The OPC server serves as a reference monitor to control access to specific security functions that are exposed by the OPC server. An OPC server may implement OPC Security in addition to DCOM Security, or implement OPC Security alone.

Role and User-Focused Security

The OPC Security specification focuses on client identification by using trusted credentials to determine access authorization decisions by the OPC server. It enables OPC products to provide specific security controls on adding, browsing, reading and/or writing individual OPC items. Within the plant environment different job roles require different types of data access:

- Control system engineers might require full read and write access to all points in the automation system

- Operators might be restricted to only those data points associated with the status and control of machines within their particular plant unit

- Management level personnel would most certainly only require read access to key performance data items

Applying the most appropriate security access means applications must be able to understand the context in which particular users are accessing information.

While the OPC Security specification opens the door for OPC servers to make informed access decisions on a per user basis, how this information is used is left up to each OPC vendor. MatrikonOPC is the one vendor that specifically focuses on ensuring users can fully protect their OPC architectures by providing a robust OPC Security implementation that delivers security control down to the per-user-per-tag level – regardless of what vendors' OPC servers are being used.

Example:
OPC Security done right!

Based on the OPC Foundation's OPC Security specification, the MatrikonOPC Security Gateway controls what users can browse items, add them to groups, as well as perform reads and writes- on a per-user-per-point basis. Such granular control over data access helps deliver the right data to the right people and prevents accidental or un-authorized OPC data access on any OPC server.

Using the MatrikonOPC Security Gateway as the top-level OPC server, data from any of the underlying, un-secure OPC servers can only be accessed by users who had such rights granted to them by the system administrator. Such role-based security provides effective OPC-centric security that directly contributes to a system's overall Defense-in-Depth strategy.

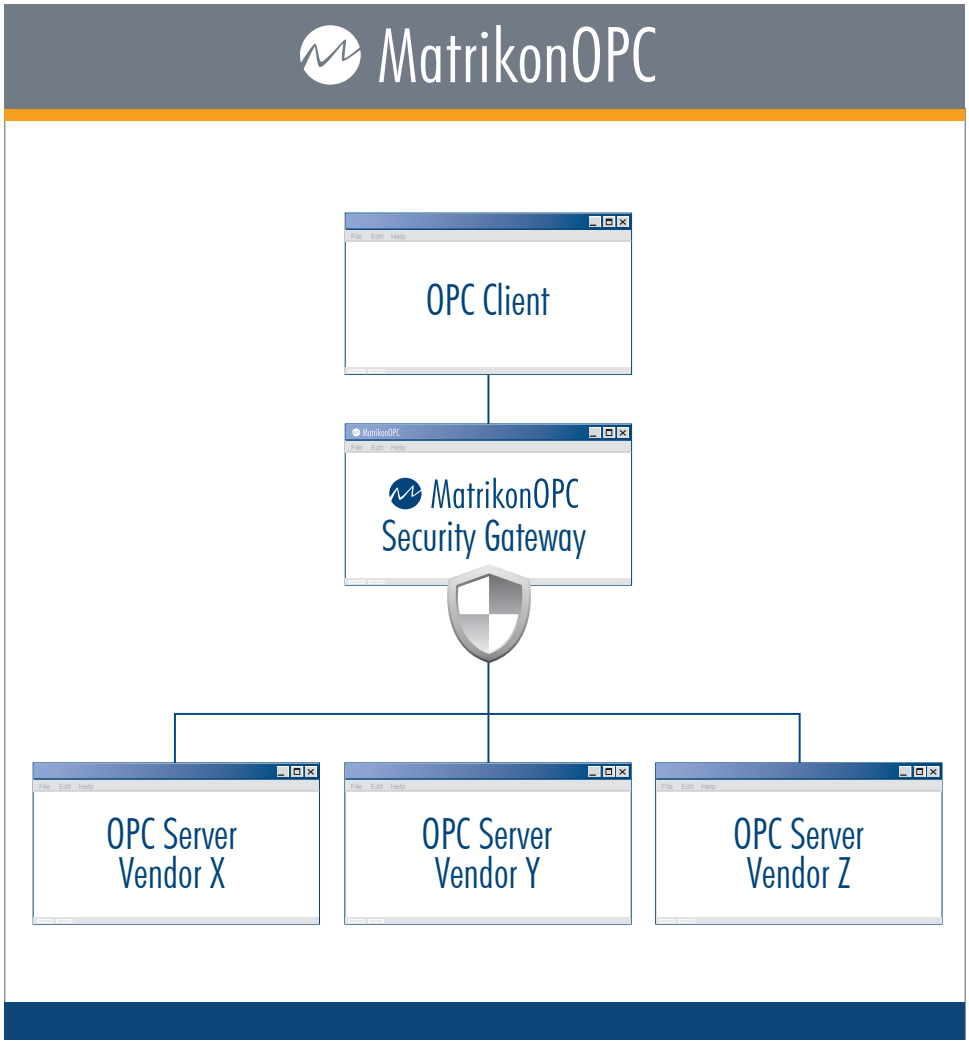


Figure 3 – MatrikonOPC Security Gateway Architecture

Type of Security	Bank	Industrial Control System (ICS)	Example ICS Defense Solutions
Network-Focused Security	Security Guards	OPC-Aware Firewall	Tofino Security Appliance and Tofino OPC Enforcer: • Tofino Security Appliances are installed to create zones of security for groups of PLCs, DCS, HMIs with similar security requirements • Installation is "plug-n-protect" requiring no pre-configuration, no network changes, and no plant downtime • Automatically tracks and manages OPC Classic's dynamic ports; and inspects, tracks and secures every connection made by an OPC application
Application-Focused Security	Tellers • Determine access to accounts, cash, vault and even to the bank manager • The effectiveness of this security layer depends on how well trained and diligent the Tellers are	OPC servers using OPC Security • Determine the level of access allowed to the OPC client application • The effectiveness of this depends on how fully the OPC security specification is implemented by the OPC server vendor	MatrikonOPC Security Gateway: • Provides comprehensive implementation of the OPC Security Specification. • Uses security data provided by the OPC Security Specification for all data access decisions – not just for initial connection acceptance. • Protects all OPC servers – regardless of what OPC vendor they are from. Allows users to secure their existing OPC infrastructures without replacing OPC servers.
Role and User-based Security	• Different Customers have different access rights to a given bank account. For example all family members may check the balance and make deposits, but not everyone can make withdrawals.	• Control engineers might have read write rights to all points in the automation system, while management has access to performance reports only	Matrikon OPC Security Gateway: • Enforces security down to the most granular level: per-user per-tag. This is the most comprehensive application of the OPC Security Specification. • Controls what users can see on any given OPC server and only allows the users to perform those actions they are cleared for.

Figure 4: Comparing defense in depth measures for banks and industrial systems

Security You Can Bank On

The implications of ignoring OPC security will grow rapidly as the demand for OPC connectivity continues to increase. History shows that the root cause behind many publicized security failures has been the result of improper use of, or the complete lack of, IT security safeguards.

Control automation professionals who are security aware use a combination of control system focused network security practices, proper OPC architecture design, and OPC–centric security products. Using the right products, the security of existing systems can be greatly enhanced without the need for replacing equipment or in-depth IT experience. The MatrikonOPC Security Gateway and the Tofino OPC Enforcer are off-the-shelf components that can secure OPC-based communications quickly and easily.

The reality is that security incidents don't just happen to 'other people'. Smart companies will prepare for the unexpected by evaluating their OPC security before a costly security incident occurs.

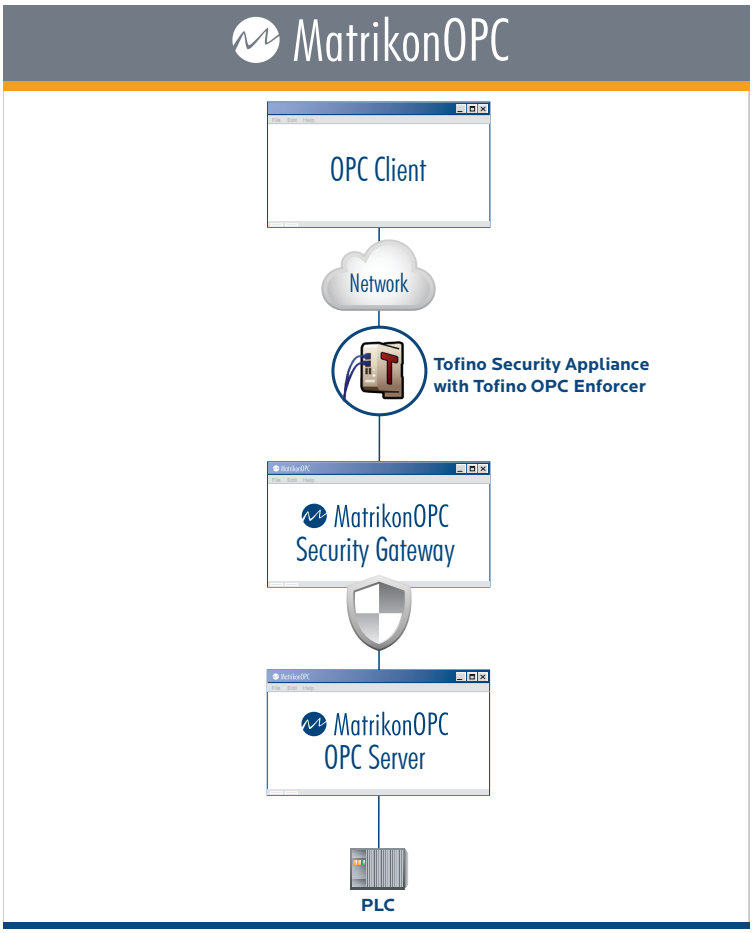


Figure 5 – Tofino & MatrikonOPC Security Gateway Solution

Next Step: Try These Solutions Yourself

MATRIKONOPC SECURITY GATEWAY

MatrikonOPC Security Gateway secures all real-time OPC architectures. Unlike OPC solutions that rely only on DCOM security, Security Gateway controls who can browse, add, read and/or write to a tag on a per-user-per tag basis on any OPC DA server. Fully standards-based for maximum compatibility, the Security Gateway implements the OPC Foundation's OPC Security specification.

Download Security Gateway

ABOUT BYRES SECURITY INC. AND THE TOFINO OPC ENFORCER

The Tofino Industrial Security Solution from Byres Security Inc. provides practical and effective Industrial Control System and SCADA security that is simple to implement and that does not require plant shutdowns.

The Tofino OPC Enforcer module provides robust security and stability for any system using OPC Classic. Unlike other firewalls, this product inspects, tracks and secures every connection made by an OPC application, opening only the exact TCP port required for a connection between an OPC client and server.

For more information, please visit www.tofinosecurity.com.

"Tofino" is a registered trademark of Byres Security Inc.

ABOUT MATRIKONOPC

MatrikonOPC provides equipment data connectivity software based on the OPC standard. The MatrikonOPC promise is to empower customers with reliable data access to all major automation vendors' systems, provide practical OPC training and deliver superior client care. MatrikonOPC builds close relationships with its customers to best address their business and technical needs. With offices in North America, Europe, Asia-Pacific and the Middle East, MatrikonOPC provides local presence on a global scale. MatrikonOPC is a vendor neutral connectivity supplier.

Toll Free: +1 (877) 628-7456
Ph: +1 (780) 945-4099
Email: info@MatrikonOPC.com
Web: www.MatrikonOPC.com