



High Security Integration Using OPC

Authors: Joe Scalia, Portfolio Architect, Invensys Operations Management
Eric Byres, Security Expert and Technical Officer, Byres Security

What's Inside:

1. The Benefits of OPC Classic
2. OPC's Soft Underbelly
3. The Search for Secure OPC Classic
4. Finally...Simple and Reliable Security for OPC
5. Fine Tuning the Triconex® Tofino™ Firewall
6. Enforcing Read-Only OPC Communications
7. References

High Security Integration Using OPC

1. The Benefits of OPC Classic

Achieving safe, reliable operation of OPC Classic implementations is well worth the effort. No single industrial communications standard has achieved such widespread acceptance across so many different industries and by so many equipment manufacturers. Once known as OLE for Process Control and now officially referred to as OPC Classic, this standard interconnects an amazing variety of industrial and business systems, ranging from human machine interface (HMI) workstations, safety instrumented systems (SIS) and distributed control systems (DCS) on the plant floor, to enterprise databases, ERP systems and other business-oriented software in the corporate world.

The reason for OPC's widespread popularity is simple: It is the only truly universal interface for communicating with diverse industrial devices and applications, regardless of manufacturer, software or communications protocol. Before OPC, developers had to create specific communications drivers for each of any of the hundreds of control systems or devices to which they desired connection. With OPC, however, they could focus on a single optimized OPC driver, which would enable connection to any OPC server, regardless of what network or controller manufacturer supplied it. This freed the end user from having to deal directly with the internal architecture of the control device. Integration teams could then work with named items (or groups of items) instead of raw register numbers and data types. This simplified adding or changing control systems, for example, easing migration from a proprietary to an Ethernet-based protocol.

OPC configuration is easier for the following reasons:

- OPC does not require intermediate data mapping that must be maintained.
- OPC provides information in its native format and syntax.
- OPC provides a universal browser to facilitate configuration.
- Named items (versus vendor specific memory locations like 40020 or N7:2) reduce the chance of human error during design, configuration and operation.

Compared to traditional communications technologies, most engineers have found that using OPC can save significant configuration time. It is rare to find an industrial facility anywhere today whose system integration strategy, at least in part, isn't based on OPC.

2. OPC's Soft Underbelly

While control system manufacturers, integrators and end users were happily deploying OPC in their plants and factories, security researchers-- and the hacking community-- began noticing snakes in this network Garden of Eden. The first and most often quoted in the popular press was that OPC Classic's underlying protocols, namely DCOM and RPC¹, can be vulnerable to attack from virus and worms. Reports such as the following indicated that the threats were real:

*"Over the past few months, the two attack vectors that we saw in volume were against the Windows DCOM (Distributed Component Object Model) interface of the RPC (remote procedure call) service ... These seem to be the current favourites for virus and worm writers, and we expect this trend to continue."*²

Even more serious, the RPC and DCOM protocols were designed before security issues were widely understood and as a result, securing OPC with conventional IT-style firewalls has been almost impossible. Unlike most other network applications, OPC servers dynamically assign TCP ports to each executable process that serves objects to clients. The OPC clients then discover the ports associated with a particular object by connecting to the server and asking which TCP port they should use. The fact that OPC servers are free to assign any port between 1024 and 65535, however, makes OPC very firewall unfriendly. Configuring an IT firewall to leave such a wide range of ports open presents a serious security hole and is thus generally considered unacceptable practice.

High Security Integration Using OPC

3. The Search for Secure OPC Classic

Initial OPC security solutions revolved around the DCOM service improvements that Microsoft included in Windows XP/SP2 and Windows Server 2003/SP1, but these soon proved inadequate. In 2006, for example, a research team commissioned by Kraft Foods Inc. and the U.S. Department of Homeland Security discovered that few engineers could actually deploy these improvements:

“Our research indicated that the most serious issue was not the protocols, but the fact that securely deploying OPC applications has proven to be a challenge for most engineers and technicians. While OPC is an open protocol with the specifications freely available, engineers must wade through a large amount of detailed information to answer even basic security questions. There is little direct guidance on securing OPC, and our research indicates much of what is available may actually be ineffective or misguided.”³

This study led to three “recommended practice” papers that outlined steps for improving OPC system security. These documents are now available to operators of critical SCADA systems on the US-CERT Control Systems site <http://csrc.inl.gov/> and at <http://www.tofinosecurity.com/articles/professional/white-papers>.

At around the same time, a number of 3rd party products that solved the multiple-port problem by tunnelling OPC/DCOM traffic over a single port began to appear on the market. Although these did make the systems administrator’s life simpler, it is not clear that they actually improved security. These designs also typically required an intermediary personal computer (PC) to manage the tunnelling. This added long-term costs, because the PCs require continual, manual patching and anti-virus updates.

In a 2008 application note, Byres Security Inc. proposed an alternative OPC security solution, this one based on managing the OPC firewall by modifying the OPC server Windows Registry settings according to a set of rules in its Tofino Industrial Firewall⁴. This solution was generally effective, but added configuration complexity for the system administrator and did not work for some poorly behaved OPC Server products.

4. Finally... Simple and Reliable Security for OPC

While tunnellers and rule-driven solutions certainly have their place, they are not enough to secure today’s most critical applications. OPC users need simpler and more robust security tools. In 2008, recognizing customer needs for greater interoperability of Triconex safety systems, Invensys Operations Management began embedding OPC servers directly within its Tricon[®] communications module (TCM). This removed the need for an intermediary PC to supply the OPC services.

It also allowed the creation of read-only access control capability client by client, something not normally possible in OPC systems. And in 2009, to ensure absolute maximum security for these embedded OPC servers, Invensys teamed with Byres Security to create a firewall that was both extremely simple to use and provably secure. The result is the Triconex Tofino Firewall, which is now available for Invensys customers using the Triconex TCM with the embedded OPC solution.

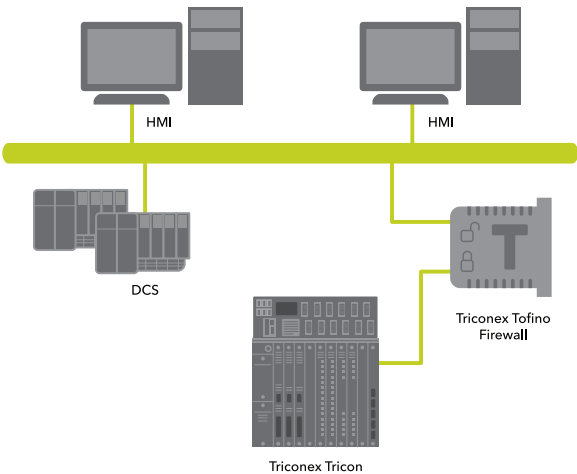
The combination of the Triconex TCM with the Triconex Tofino Firewall automatically addresses a wide variety of OPC security issues by offering multiple layers of defence:

1. A tightly closed firewall automatically tracks all the TCP ports assigned by the OPC servers for DA and A&E connections and then dynamically opens those ports in the firewall only when needed and only between appropriate client/server pairs.
2. Built-in OPC sanity checking blocks OPC session requests not conforming to the DCE/RPC standard, preventing many common malware attacks.
3. Pre-defined anti-DoS filters manage traffic levels so that traffic storms cannot impact the safety system.
4. Read/Write access control features in the TCM allow complete lockdown of what devices can read or write to the safety system.



Figure 1: Triconex Tofino Firewall and Triconex Tricon Controller

High Security Integration Using OPC



End-user staff without network security experience or training can implement all of these state-of-the-art security features easily. The firewall is pre-configured at the Triconex factory so it can operate in most Triconex installations without adjustment. Users simply insert it in-line between the control network and the Ethernet port on the Triconex Communications Module as shown in Figure 2.

Installation of the firewall is also extremely simple. It accepts a wide range of DC voltages, ranging from 9 VDC to 32 VDC, so common instrument power supplies can be used to power it. And field technicians need deal with only the following two Ethernet interfaces:

1. A lower (“trusted”) interface, which is labelled with a “closed” padlock symbol and connects to an Ethernet interface on the TCM where the OPC server resides.
2. An upper (“untrusted”) interface, which is labelled with an “open” padlock and connects to the rest of the control network (DCS, HMI, etc) where the OPC clients reside.

Figure 2: A Secure OPC Network for Safety Systems

There are no DIP switches to adjust, no serial cable to connect and no IP addresses to set. Once the firewall is installed and powered up, the field technician can simply walk away.

The firewall inspects all network traffic destined for the TCM and the OPC server and blocks any potentially harmful traffic before it can reach the TCM. The Triconex Tofino Firewall also provides the following additional security features:

- Rate limits are applied to all incoming traffic to ensure that the TCM cannot be disrupted by traffic overload conditions.
- All OPC connection requests are “sanity checked” for compliance with the RPC protocol specification; they will be blocked if non-compliant.
- The Triconex Tofino Firewall logs of all exception conditions that it detects, including blocked network traffic. These log entries may be saved to a USB storage device for inspection using a standard text editor.

5. Fine Tuning the Triconex Tofino Firewall

Most firewalls require a detailed knowledge of complex Access Control List languages or expensive programming systems. Making matters worse, studies have shown that the complexity of most firewall configurations can result in errors that effectively leave the system wide open to attack⁵.

To address this possibility, all security configurations are automatically defined using the TriStation software supplied with all Triconex systems. For example, in some installations, the Triconex Communications Module will be configured to use custom TCP and UDP port numbers for Modbus TCP. In these installations, the Triconex Tofino Firewall must be re-configured to use the same port numbers; otherwise, the firewall will block any network traffic using these customized port numbers. The Triconex Tofino Firewall makes this task simple:

1. The TriStation software exports the standard TCM configuration data into an XML file.
2. The Triconex Tofino Configuration Utility reads this XML file and saves a set of encrypted firewall configuration files onto a USB memory stick, based on the actual TCM settings.
3. Users load the encrypted configuration files by inserting the USB storage device into the firewall.

Once this simple procedure is performed, the custom configuration will be permanently stored in the firewall.

6. Enforcing Read-Only OPC Communications

The Triconex TCM Access List feature permits the user to limit access to the Triconex SIS to specific devices on the control network, and also to restrict the type of access by protocol. For example, OPC clients can be limited to read-only access. By combining access control with the Triconex Tofino Firewall, the user can quickly and easily implement multi-layered 'defence-in-depth' protection for the SIS.

Of course OPC Classic might not be the only protocol that needs to pass through the firewall, so the system is extensible to also allow Modbus TCP, Simple Network Time Protocol (SNTP), the Triconex management protocols, network printer access and ICMP ("ping") traffic. These protocols are allowed by default, but will be disabled by the firewall configuration utility if they are not active in the TriStation configuration file. This provides an extra level of security by blocking network traffic that is not required for correct plant operation.

7. Summary

The Triconex Tofino Firewall is the first true OPC Classic security solution designed with the needs and skills of the control technician in mind. There are absolutely no configuration changes required on the OPC clients and servers and it offers superior security over what can be achieved with conventional firewall or tunneler solutions. It is designed to automatically interpret standard TriStation controller export files and create refined firewall rules without any special training. Combined with the TCM access list features, the Triconex Tofino Firewall creates the ideal defense-in depth solution for better safety integrated system reliability and security.

8. References

¹ Many readers will be aware that the OPC Foundation is developing a new version of OPC (called OPC Unified Architecture or OPC-UA) that is based on protocols other than DCOM. Once most OPC applications migrate from the DCOM-based architecture to .NET-based architectures, it is likely that they will enjoy greater security and reliability. Unfortunately, all indications are that it may be many years before most facilities actually convert their systems.

² Bruce Schneier, "Attack Trends" QUEUE Magazine, Association of Computing Machinery, June 2005.

³ Eric Byres, Matthew Franz, Dale Peterson, and Joel Carter; OPC Security Whitepaper #1 - Understanding OPC and How it is Deployed

⁴ "Application NoteAN105: Securing OPC Traffic with a Tofino Security Appliance"; Byres Security Inc, December 2008

⁵ Avishai Wool, "A quantitative study of firewall configuration errors" IEEE Computer Magazine, IEEE Computer Society, June 2004, Pages 62-67

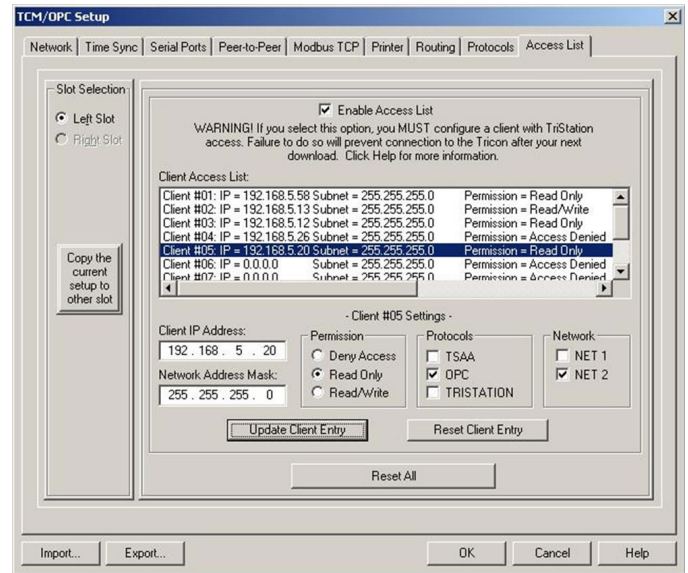


Figure 3: TCM Access List settings controlling which clients get Read/Write versus Read-Only OPC access