OPCNet Broker™ for Industrial Network Security and Connectivity

Tunneling Process Data Securely Through Firewalls

A Solution To OPC - DCOM Connectivity from Integration Objects
Compatible for DA, HDA and A&E

Table of Contents

Table of Figures

About Integration Objects

Integration Objects is a leading provider of OPC software products for industrial automation solutions. Their OPC software products are employed in a variety of industrial environments, including process plants, pipelines, electrical grids, transportation infrastructures and utility equipment. Using the most advanced Microsoft development technologies, Integration Objects' products are highly scalable and specifically designed for security, reliability, and interoperability with the lowest overhead computing. Details about Integration Objects can be found on the web at www.integ-objects.com.

About OPCNet Broker™

OPCNet Broker ™ (ONB) ensures fast, reliable, and secure OPC remote communication by overcoming DCOM bottlenecks. The ONB is an easy-to-deploy and maintainable solution that allows:

- Process Control and SCADA Network Security down to the tag level,
- Tracking of client/server communications,
- Limiting the number of open ports within firewalls to minimize security holes,
- Configuring the communication schema with less complexity,
- Connecting OPC components from different domains, through both LAN and WAN networks.

Summary

Manufacturing companies have invested billions of dollars in industrial automation infrastructures, but many have not yet realized the full value from their investments as many of these investments remain islands of automation, disconnected from other systems- including business systems.
The question of whether to integrate between process controls, the plant-level and enterprise systems is no longer a question up for debate if manufacturing and energy companies want to remain competitive. However, the sharing of process information within and between networks must be done in a way that aligns with the overall security policies of the enterprise. That is the role of Integration Objects' new OPCNet Broker™ (ONB). ONB provides the secure transfer of process data, even across multiple firewalls, Network Address Translators (NAT) and WAN networks. To not securely transmit process data exposes process control networks to potential cyber attacks which can disrupt production, compromise safety and cause significant financial losses for companies. This paper expands on the issues and challenges of using DCOM when deploying OPC technology and presents an alternative solution that addresses the industrial end-user requirements.

Most of these industrial users have standardized on OPC as their backbone for all industrial connectivity solutions, thus enabling interoperability between multi-vendor systems and devices.
Deployment of OPC-based applications is easy when both clients and servers are installed on the same machine. It becomes somewhat more challenging when both systems are installed within the same process control network, but on two separate machines. Such configurations are possible and present little security risk when left like that. However, with a two computer configuration, challenges arise when attempting to connect a process control network to an enterprise or business network(s). These challenges are primarily due to the fact that OPC specifications are originally based on COM/DCOM which is difficult to implement and presents security vulnerabilities.

Users' concerns about DCOM including the difficulty of configuration, robustness, integrity of the data, and performance of the data transfer are repeated themes from the industrial community. This is best understood from the following details. Users face major challenges configuring DCOM when the server and the client are installed remotely on two separate machines. Most hotline support issues related to DCOM are configuration challenges, which can consume days to weeks in troubleshooting. Configuration challenges are heightened substantially when servers and clients are on two different domains, or have a firewall in between them. Another concern that is often raised by industrial end-users is the way DCOM enables security lapses and the associated

impact on the integrity of the process control data.

This document…

- Enumerates the DCOM challenges,
- Presents the most suitable replacement technology,
- Compares .Net Remoting technology with DCOM,
- Offers a flexible architecture with .Net Remoting,
- Provides a solution and proposed architecture that addresses the security issues.

User Challenges with DCOM

About DCOM and Security

Distributed COM (DCOM) is a Microsoft proprietary technology that was designed for general IT (back office) applications. Developed from a general IT perspective and not real-time process control, the vulnerabilities of DCOM are well-understood, both inside and outside the process control community. Most of the support calls that OPC product manufacturers receive are due to the DCOM set-up configuration challenges that end-users face. We attribute this issue primarily to the complexity of setting up DCOM and Windows Security.

For example, DCOM requires many ports for finding other hosts, resolving names, requesting services, authentication, sending data, and more. If these ports are not available, DCOM will automatically search for others. Any port and service used by DCOM is a target for viruses and worms. A capable hacker can create services directed at these ports that query which services are running and that match the hacker's toolkit of exploit scripts. For example, Port 135 must be open for the initial communication handshake, plus an additional range of ports whose numbers depend on the quantity of running processes hosting DCOM objects. The default port range is typically large, although it can generally be reduced. DCOM makes dynamic port allocations, i.e. it chooses random ports numbered beyond 1024 while opening connections.

DCOM also cannot work across Network Address Translation (NAT). Callbacks are not carried out on the same port (but a new one is opened). This means that when a callback is set up, the client and server roles are reversed so that the firewall sees the server as a client trying to open a network communication to the outside—and this will likely fail in a default firewall configuration.

About DCOM Robustness

DCOM can take an unreasonably long time to fail an activation request as it tries each available network protocol (TCP, UDP, IPX, NP, etc.) one after the other, until they all fail. Timeouts of 3 minutes are not uncommon (The DCOM designers claim they chose robustness over performance, but that contention is unsupportable.). Few IT users will want to wait 3 minutes for an LAN connection to respond -- 3 seconds is more like it! (Ref: http://www.windojitsu.com/code/atlxdcom.h.html)

Set-up complexity

Set-up configuration can be best managed when both OPC clients and servers are installed on the

same machine. The challenges start when both systems are installed remotely, configured as NT services, or running over a WAN. To perform such a configuration, the user has to be an expert on Windows Security. The set-up can be very complex and it could take weeks for some users, even with a lot of assistance, to get the connectivity between the OPC clients and servers working.

OPC based software technology is now available to help avoid DCOM challenges when trying to send process data and messages from one system to another, while still ensuring fast, reliable, and secure OPC remote communications. Integration Objects' OPCNet Broker™ for DA, HDA and A&E is one such example.

These tools are typically easy-to-deploy and maintainable solutions that allow:

- Easy and quick set-up, with only a few clicks needed,
- Tracking of client/server communications,
- Tunneling across firewalls through single ports to minimize security holes and Network Address Translators (NAT),
- Connecting OPC components from different domains, across VPN and through WANs and LANs,
- **User authentication at the server and tag levels** for increased security,
- Automatic reconnection when the connection is lost,
- Configurable communication timeouts,
- Data encryption for security reasons,
- Data compression for better performance of data transfers across the network.

OPCNet Broker™ uses a message queue that is a queue (repetition) of all messages that are to be sent through a specific transport connection. The message queue is necessary only for messages' being sent and only if the connection is currently unavailable for sending. Constraints can be applied to the maximum size of messages being sent, to the total size of all messages kept in the queue and to the total number of messages kept in the queue.

OPCNet Broker™ also uses a compression algorithm. The compression ratio is highly dependent on the content being sent. Usually, using the compression feature reduces traffic by 5-10 times for large text and Data Set values. In general, English text in the ASCII format is usually compressed by a factor of 2.5 to 3. UNICODE text is usually compressed by a factor of 4 to 6. This significantly increases the ratio of compression. Integration Objects chose to build its OPCNet Broker™ solution around .Net Remoting with the relevant configuration to address the specific requirements of the OPC communications and process control network security.

Solution Description – Examples

This section describes a solution based on two OPCNet Broker™ licenses, one on the server side and the other on the client side. These two gateways are built around the OPC client and server. They act as .Net peers and communicate through .Net Remoting. Their role is to redirect COM (and .Net) calls to .Net (and COM) calls.

.Net Remoting Architecture

The OPC Server and Client in Figure 1 are isolated by a firewall. To communicate with each other, they need to select the same channel protocol and formatter. Formatters are the objects that are used to encode and serialize data into messages before they are transmitted over a channel. At the other end of the channel, when the messages are received, formatters decode and de-serialize the messages. Channel protocols include TCP and HTTP. Formatters include SOAP and binary. For the best performance, we recommend using the TCP channel with a binary formatter.

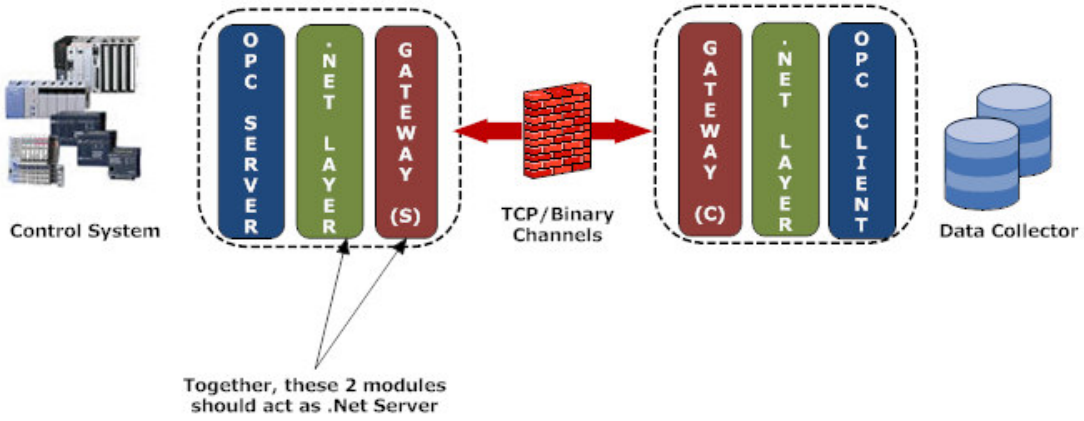

Figure 1: OPCNet Broker™

To access a server, the client just needs to specify the server's IP address and the port on which the server will listen. It can get such information from a configuration file (XML file for example).
And as said above, bidirectional communication on a unique port is possible. Here the .Net Remoting architecture provides a way for applications on different machines/domains to communicate with each other and offers a powerful, yet easy way to communicate with objects in different app domains. So, .Net Remoting communications can traverse different domains and

overcome domain controllers' security policies. Security barriers can be set using SSPI (authentication, etc.) or other custom developed modules.

Communication through Firewalls and Domains

Figure 2 illustrates a second configuration example that shows the communication of process data between two domains, each behind a dedicated firewall.

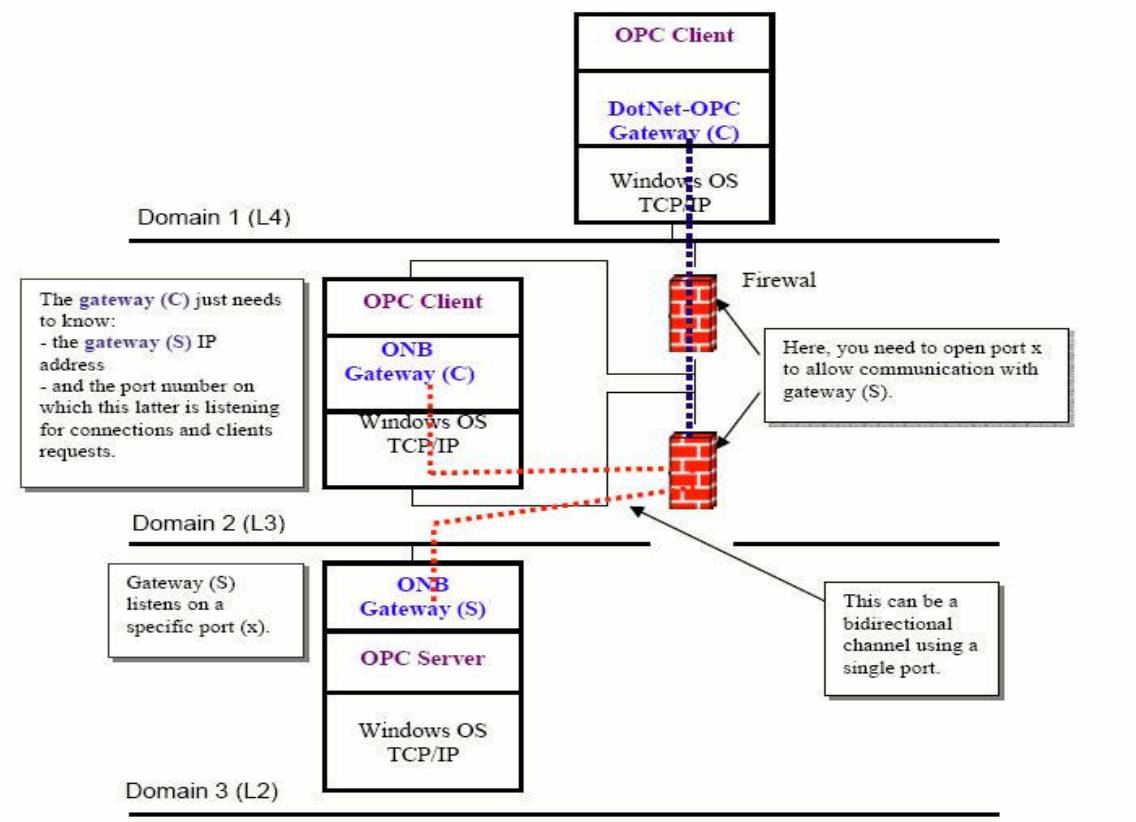

Figure 2: OPCNet Broker™, 2nd Configuration

ONB through VSAT Communications

VSAT (Very Small Aperture Terminal) networks offer value-added satellite-based services capable of supporting the Internet, data, video, LAN, voice/fax communications, and can provide powerful, dependable private (LAN) and public (WAN) network communications solutions. They are becoming increasingly popular because VSATs are a single, flexible communication platform that can be installed quickly and cost effectively to provide telecom solutions for consumers, governments, corporations and industrial sites.

The benefits of VSAT technology are being realized in many sectors, both private and public. From banks to administrations, schools, hospitals, and rural telecommunications, VSATs are being seized upon to elevate economic, educational, and health standards.

The VSAT Applications are common and often necessary in the industrial networks and include:

- **Interactive Data:** Corporate networks, point-of-sale terminal to host, inventory checks, financial data transfer and process control.
- **System Control and Data Distribution:** Corporate networks, process control, pipeline monitoring and flow control, resource monitoring and control, and electric power grid control.

However, considering the nature of the process control network, using OPC over satellite communications represents several challenges:

- Security Concerns: Even though VSAT is now considered as a secure and reliable medium to connect geographically dispersed locations, there are still several ways that satellite systems can be disrupted. With sufficient power from a satellite dish on the ground, an orbiting satellite's signal can be blocked.

  Industry sources and experts claim that many of the potential pitfalls are not restricted to satellites as the problem source. Smaller radio stations have been known to have their signals blocked by more powerful transmitters. And hackers could just as easily attempt to break into the computer systems of a cable operator in an attempt to shut down services to a certain neighborhood.

- Outages due to weather: VSATs are subject to signal attenuation due to weather ("Rain Fade"); the effect is typically far less than that experienced by one-way TV systems that use smaller dishes, but is still a function of antenna size and transmitter power and frequency band.

- Occasional outages due to the sun: Twice a year, there are brief periods (lasting a few minutes) where the Sun moves directly in line with the satellite. The Sun, being a very powerful source of radio signals, temporarily jams the satellite signal. These outages can be predicted very precisely and last only a short time.

Using the OPCNet Broker™, instead of DCOM to establish the communication between the OPC Clients and Servers, will overcome these limitations. In fact:

- Using VSAT communications always requires the implementation of firewalls. OPCNet Broker will make this implementation very easy since it uses one single port.
- OPCNet Broker introduces additional levels of security using the data encryption and the user authentication features.
- The ONB automatic reconnection mechanism will automatically reestablish the connection between the OPC clients and servers. Per the user's configuration, this mechanism will either try to reconnect indefinitely or to reconnect over a limited number of times.

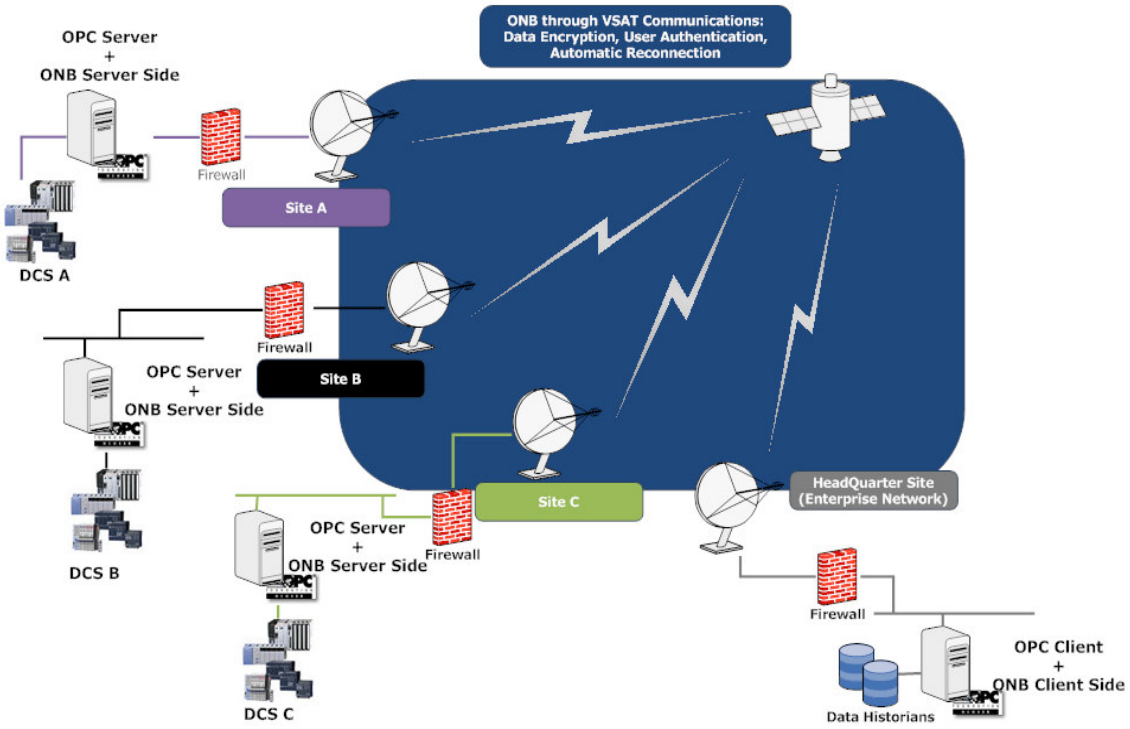

Figure 3: OPCNet Broker™ through VSAT Communications (Financial Data Transfer Application)

Conclusion

The integration between business (enterprise) systems and production systems can increase the visibility of the manufacturing supply chain and create a more agile business environment. Such integration requires the transmission of process data values across firewalls, where security considerations are essential. While the OPC standard is useful in this application, OPC and DCOM together can pose challenges when implementing and maintaining. This paper has presented a new technology called OPCNet Broker™ that is OPC DA, HDA and A&E compatible and that employs the OPC communication standard without the need for DCOM. The technology increases the security of data and the overall usability of the solution. In summary, OPCNet Broker™ facilitates the integration between and with production systems - from the single plant system level to highly complex networks; while still preventing cyber attacks and unauthorized users from gaining access to critical process control data and the systems that manage production.