DataWorX32
OPC Tunneling

October 2015
An ICONICS Whitepaper
www.iconics.com

Visualize Your Enterprise™

CONTENTS

1 About This Document

1.1 Scope of the Document

This document contains information on the features of the ICONICS OPC Tunneling product that may be of use to companies wishing to network OPC clients and servers running on different platforms, in different domains, or in completely separate networks. An overview of OPC Tunneling in general and on the DataWorX32 implementation of OPC Tunneling is presented.

The intended audience includes engineers working on implementing OPC communications over wide area networks and sales and marketing personnel desiring to gain an understanding of the product features of DataWorX32 OPC Tunneling.

1.2 Revision History

Version 9.0 – Dave Oravetz, July 22, 2006 (initial release)

1.3 Definitions

The following are acronyms used in this document, and are presented here for reference.

- COM – (Microsoft's) Component Object Model
- DCOM – (Microsoft's) Distributed Component Object Model
- DCS – Distributed Control System
- HMI - Human Machine Interface
- I/O – Input / Output
- LAN – Local Area Network
- OPC - OLE for Process Control
- OPC DA – OPC Data Access
- OPC A/E – OPC Alarms and Events
- OPC HDA – OPC Historical Data Access
- PLC – Programmable Logic Controller
- SCADA - Supervisory Control and Data Acquisition

2 Introduction

OPC Communications has become the de facto standard for data exchange between industrial automation applications. Originally based on Microsoft's OLE COM (Component Object Model), and DCOM (Distributed Component Object Model) technologies, OPC communications quickly became widely adopted by DCS (Distributed Control System), Factory Automation, Building Control System, and other industrial automation vendors over the past ten years. It has proven to be secure, reliable, easy to use, and truly inter-operable. As a result, it has provided significant cost savings to end users, eliminating the need for them to develop expensive custom software and applications when integrating components from multiple vendors into a single system.

While the original COM/DCOM-based OPC standards have served industry well, there are limitations to its use. The most notable is the reliance on DCOM for remote communications. The most common complaints related to DCOM are the complexity to configure DCOM, that DCOM is not real-time (it can take approximately 6 minutes to detect and notify when a failed connection has occurred), and that DCOM is not firewall friendly (to pass through a firewall requires the user to open many ports on the firewall, severely compromising the security features of the firewall).

Some of the larger automation system and SCADA system vendors have worked around the limitations of DCOM based OPC communications by developing and using their own proprietary communications to move data around within their system. These systems convert the OPC data to a proprietary format at the remote (OPC Server) location. A drawback to this approach, from the user's point of view, is that there are locked into using the particular vendor's communications technologies. The user's options are limited to architectures, security models, and flexibility supported by the particular vendor, and of course by the prices the vendor decides to charge.

Choosing to base their communications strategy on the core OPC standards, other SCADA vendors, including ICONICS, Inc., have adopted approaches were the OPC communications is "tunneled" within other communications layers or technologies. This has proven to be a very effective approach that both eliminates the need for DCOM, and provides for a more open communications system, and one that continues to evolve and improve as the OPC standards continue to evolve and improve.

New with the V9 release of ICONICS DataWorX32, ICONICS is introducing a standalone OPC Tunneling product that is based on the industry proven ICONICS GenBroker communications. The DataWorX32 OPC Tunneling product advances the state-of-the-art of OPC Tunneling products in that it supports all three major OPC Standards (OPC DA, OPC AE, and OPC HDA). Furthermore, it supports new advances in OPC Tunneling security, based on the new OPC UA standards, where the user's credentials are passed to the server side of the tunnel for authentication. More details of these features and other features of DataWorX32 OPC Tunneling are described in this paper.

3 DataWorX™32 OPC Tunneling

3.1 DataWorX32 OPC Tunneling Overview

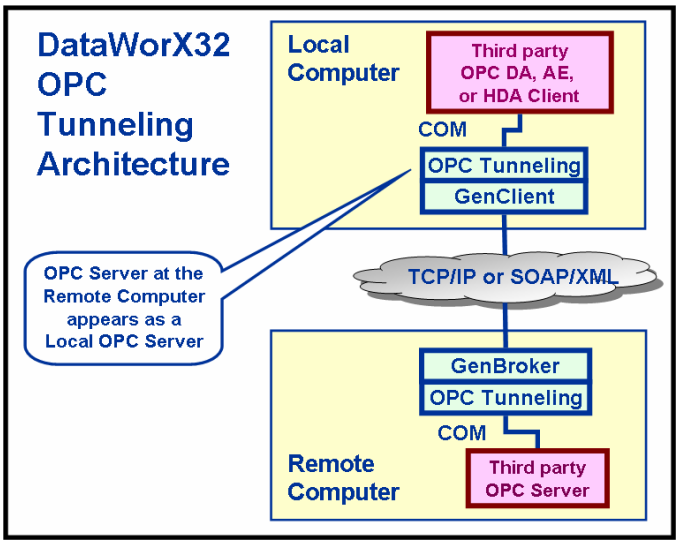
ICONICS DataWorX32 OPC Tunneling provides a safe, secure way to extend your OPC communications network greater distances, through network firewalls and address translators, and across network domains. It is based in the industry proven ICONICS GenBroker communications technology. Similar to other OPC tunneling products on the market, DataWorX32 OPC Tunneling "tunnels" the OPC COM-based communications through various network topologies without the use of DCOM.

While other tunneling products offer TCP/IP, DataWorX32 OPC Tunneling offers a choice of communications protocols that include TCP/IP and the more firewall-friendly SOAP/XML protocol. The DataWorX32 OPC Tunneling also provides an additional level of security not found in other tunneling products. Based on the new OPC Unified Architecture (UA) technology, DataWorx32 OPC Tunneling provides an option to authenticate the communications to each remote OPC Server. This is done by passing the User's Credentials to the remote server location, and verifying the user has the rights to access the remote OPC Server.

3.2 DataWorX32 OPC Tunneling Architecture

DataWorX™32 OPC Tunneling connects remote OPC servers to a local computer. It supports third-party OPC server to third-party OPC client communications. DataWorX™32 Tunneling fully supports the OPC Foundation's latest Data Access (DA), Historical Data Access (HDA), and Alarm and Events (AE) specifications.

DataWorX32 OPC Tunneling, which comes as a standard part of all DataWorX32 V9 products, connects a remote OPC server to a local client in a robust and secure manner, allowing for one server to be redirected to more than one user location. The powerful graphical interface allows for easy place to configuration and a centralized manage all remote connections. The underlying technology behind OPC Tunneling is the patented ICONICS



GenBroker™ communication, which provides high-performance and robust communication, providing an alternative to conventional Microsoft DCOM communications. OPC Tunneling is completely OPC-compliant and IT firewall-friendly, supporting communications over LANs, WANs and the Internet with extensive built-in security.

3.3 DataWorX32 OPC Tunneling Features

The DataWorX32 OPC "tunneling" technology is simple to install and deploy to virtually any application requiring remote and secure OPC communications. DataWorX32 OPC tunneling fully supports the latest open OPC industry standards, including:

- **OPC Data Access 3.0**
- **OPC Alarm and Events 1.1**
- **OPC Historical Data Access 1.2**

Other significant features of DataWorX32 OPC Tunneling include:

- Auto-discovery of remote OPC DA, AE and HDA servers
- Simple to set up and configure
- Supports OPC browser interfaces over LANs, WANs and the Internet
- Provides a robust, secure alternative to standard Microsoft DCOM communications
- Integrated secure communications
- IT-friendly communications through firewalls and Network Address Translators (NAT)
- Supports TCP/IP and SOAP/XML communication protocols

3.4 DataWorX32 OPC Tunneling Security

DataWorX32 OPC Tunneling provides a level of security typically not found in other tunneling products. DataWorx32 OPC Tunneling uses new technology developed as part of the OPC UA standard, to authenticate the communications to each remote OPC Server. This is accomplished by passing the User's Credentials (User name, Domain name and password) to the remote server location. To ensure privacy and security, these credentials are encrypted. The server side of the OPC Tunnel uses the credentials to obtain authentication, and uses impersonation to create the server under the specified user account. This ensures that not just any tunneled client can start up and access a remote OPC Server, only those that have the authorization can do so.

Each OPC Tunneling connection can have its own set of credentials. The credentials can be pre-configured by the user, or the user can be prompted to enter the credentials when starting up the

client application. A built in cache allows the system to remember the user-entered credentials, so that the user does not have to repeatedly enter their credentials.

If the specified User does not have the proper access rights to the remote OPC Server, then the OPC Tunneling creation fails, and an “Access Denied” error is reported. The access is controlled by the DCOM Configurator at the remote location. The Default Access permissions or Server Specific permissions may be used.

4 Summary

The ICONICS DataWorX32 OPC Tunneling technology provides a elegant and unique solution when trying to connect any complaint OPC Server to an complaint OPC Client over a LANs, WANs and the Internet.

Microsoft DCOM has presented a level of complexity that the average user has been having since its introduction. The DataWorX32 OPC Tunneling technology eliminates DCOM altogether. DataWorX32 also eliminate the long 6-minute DCOM timeouts that can effectively shutdown applications.

DataWorX32 OPC Tunneling is a simple-to-deploy, high scalable and easily maintainable solution with the following capabilities:

- Connect OPC Clients and Servers from different domains.
- Simple and quick Configuration
- Patented Data Aggregation for greatly improved Network Communications
- Data integrity by using Secure encryption/decryption technology
- Support for required and most Optional OPC Data Access interfaces
- Support for required and most Optional OPC Alarm & Events interfaces
- Support for required and most Optional OPC Historical Data Access interfaces
- Track client/server communications and limit the number of open ports within your firewalls to minimize security holes.
- Configure your communication schema with less complexity
- Accessibility for clients behind NAT, firewall and proxy
- Guaranteed and Configurable DCOM timeout
- Data transmission in a secure mode
- Automatic reconnection incase of network anomalies
- User authentication to avoid unauthorized access
- Selectable Protocol using TCP/IP or SOAP / XML
- Supports OPC Browse Interfaces

In summary, if your project requires OPC communications across networks as well as the internet then DataWorX32 OPC Tunneling will quickly solve all your remote connectivity requirements.

Founded in 1986, ICONICS is an award-winning independent software developer offering real-time visualization, HMI/SCADA, energy, fault detection, manufacturing intelligence, MES and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70% of the Fortune 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality and be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil & gas, renewable energy, utilities, water/wastewater, pharmaceuticals, automotive and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity and excellence in product design, development, technical support, training, sales and consulting services for end users, systems integrators, OEMs and Channel Partners. ICONICS has over 300,000 applications installed in multiple industries worldwide.

World Headquarters
100 Foxborough Blvd.
Foxborough, MA, USA, 02035
Tel: 508 543 8600
Email: us@iconics.com
Web: www.iconics.com

European Headquarters
Netherlands
Tel: 31 252 228 588
Email: holland@iconics.com

Czech Republic
Tel: 420 377 183 420
Email: czech@iconics.com

France
Tel: 33 4 50 19 11 80
Email: france@iconics.com

China
Tel: 86 10 8494 2570
Email: china@iconics.com

Italy
Tel: 39 010 46 0626
Email: italy@iconics.com

UK
Tel: 44 1384 246 700
Email: uk@iconics.com

India
Tel: 91 22 67291029
Email: india@iconics.com

Germany
Tel: 49 2241 16 508 0
Email: germany@iconics.com

Australia
Tel: 61 2 9605 1333
Email: australia@iconics.com

Middle East
Tel: 966 540 881 264
Email: middleeast@iconics.com

Microsoft Partner
Gold Application Development

Microsoft Partner
2014 Partner of the Year Winner
Public Sector: CityNext

64™ | Windows 8 Compatible | Windows 10 Compatible | Windows Server 2012 Certified | BTL | CERTIFIED OPC | vmware READY

VISUALIZE | ANALYZE | MOBILIZE | CLOUD

www.iconics.com