Matrikon®

Matrikon® OPC DMZ Agent™
Datasheet

Secure Control Automation Data Sharing Across Firewalls and DMZs!

Firewalls and De-militarized Zones (DMZs) are common and effective IT security tools for managing network access throughout the enterprise. For this reason, they are used by virtually all production and manufacturing facilities to maximize operational cyber security.

While correctly implemented DMZs help protect control automation data sources, they can make it difficult for valid outside users to access the data they need because systems outside of the DMZs are not authorized to establish connections through the DMZs.

Use the Matrikon® DMZ Agent to quickly and easily overcome the DMZ obstacle without compromising any security policies nor exposing your important data sources to additional risks.

Built using standardized, commercial off the shelf (COTS) Matrikon® applications, DMZ Agent is easy to setup and provides a rich set of functions including:

- Complete OT administrative control of what is shared by data sources on the shop-floor
- Support for both OPC Classic and OPC UA data connectivity
- Firewall friendly data transfer methods approved by IT departments world wide
- Enables you to share real-time and Historical data and works well with 3rd Party historians
- Isolates your data sources from direct access by users outside of the DMZ
- Protects your data confidentiality and integrity via encryption
- And more

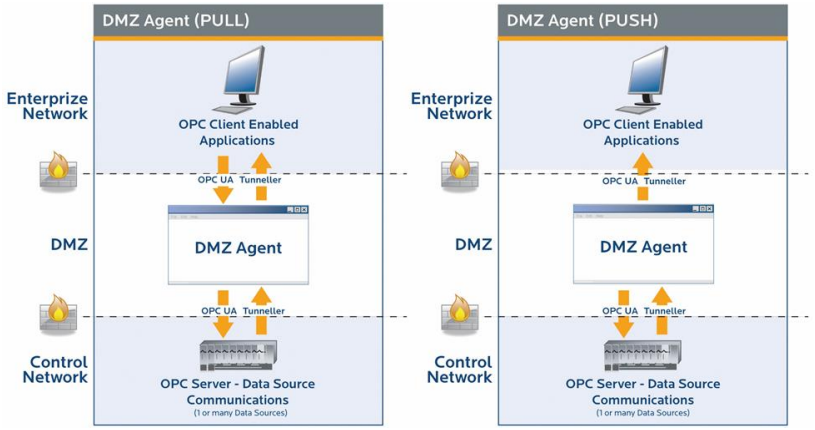
Matrikon® OPC DMZ Agent™ provides a secure, standardized solution for accessing real-time and archived control automation data across De-Militarized Zones (DMZs) using off the shelf Matrikon products.

Problem: Corporate IT departments implement DMZs to protect network assets by layering and isolating secure zones form those that are considered less secure.

Network traffic is restricted between these layers via multiple firewalls and a common PC between them. While DMZs work to secure the automation environment from the dangers present in the outside world, they prevent necessary option and business applications from accessing key day and using traditional methods.

Solution: DMZ Agent™ overcomes DMZ related control data sharing issues by providing engineers and system integrators with two time-tested OPC architectures depending on design and corporate security policies.

- DMZ Agent Pull solution enables permitted enterprise applications to securely initiate requests for OPC data located within a secure network.
- DMZ Agent Push solution allows permitted enterprise applications to receive secure network data pushed from with a DMZ (one way firewall configuration).



FEATURES & BENEFITS

- Streamlined architecture provides flexible configuration depending on data needs.
- Easy to use, requires minimal configuration and maintenance.
- Eliminates traditional DCOM and firewall issues associated with DMZs
- Provides secure, controlled access to process data.
- Enables access from multiple data sources to multiple users
- Works across multi-layered networks.
- Push architecture provides access to historical data.
- Pull architecture provides access to real time and/or historical data.
- Pushes data to an archive outside the DMZ or allows OPC Clients to pull data from DMZ.
- Integrates with all historians and databases.
- Configurable data encryption.
- OPC UA compatible

SYSTEM REQUIREMENTS

Operating Systems:

- Microsoft Windows XP Pro SP3
- Microsoft Windows 2003 Server
- Microsoft Windows 2008
- Microsoft Windows 7

Hardware Requirements:

- Intel® Core™2 Duo Processor
- 4 GB RAM
- 80 GB 7200 RPM Hard Drive

Supported OPC and OPC UA Specification

- OPC DA (OPC Data Access) 2.05a
- OPC HDA 1.20
- OPC UA DA