OPC for Industrial Control Systems
• Introduction to industrial connectivity
• Classic OPC: OPC-DA
• Overcoming limitations: OPC-UA.
• Tunneling functionality
• Connectivity Platform
• Example of an Oil and Gas / Petrochemical application
• Example of a Pharma application
INTRODUCTION TO
INDUSTRIAL CONNECTIVITY
BEFORE OPC

- Each application, its own driver
- Little integration between systems
- Proprietary solutions

Where is my data?
Adapt to changes?
THE OPC SOLUTION
THE OPC SOLUTION
OPC-DA
OPC-DA FEATURES

• Public specification, not proprietary
• Client-Server Architecture
• Data sent as plain text
• Real-time Value, Timestamp and Quality (VTQ)
• Based on Microsoft ActiveX and COM/DCOM

Note: The client is managing the server, telling it what actions to complete. If no client is connected, the server does nothing!
OPC DA LIMITATIONS

• Dependent on Microsoft’s Distributed Component Object Model (DCOM)
• Authentication controlled through Windows Component Services, not any 3rd party software product
• Microsoft Windows Domain or Workgroups only
• Inside firewall
• OPC DA over VPN access is not possible
OPC-UA
OPC UA

- Considered the future of OPC and gaining popularity

**Purpose:** Provides a single, secure, and reliable cross-platform framework for access to real-time, historical, alarm and event data

**Features:**
- Combines classic OPC specifications such as OPC DA, OPC HDA, and OPC AE into a single unified protocol
- Designed to be Internet-ready, firewall-friendly, and very secure
- Does not rely on proprietary Microsoft technology (No DCOM or WCF)
- Two types of transport: Binary over TCP, or SOAP/HTTP over TCP
- Allows support for Windows and non-Windows OS
OPC-UA REMOTE COMMUNICATIONS

- Endpoint to endpoint communication through a single dedicated TCP port (very easy to get through network barriers)

- Data encryption to RSA standards and authentication based on the x509 Certificate standard. (This is the same encryption eCommerce uses)

opc.tcp://10.10.110.10:49320
SECURITY IN OPC-UA

– Authentication and Authorization
  • Certificate Exchange
  • User/Password

– Integrity
  • Signed Messages

– Confidentiality
  • Encrypted Messages

Secure Communications in non-secure environments
Direct communications from Enterprise level to plant-floor
### COMPARE OPC DA TO OPC UA

<table>
<thead>
<tr>
<th>OPC DA and DCOM</th>
<th>OPC UA and Binary/TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applications typically must reside on the same network</td>
<td>• Applications may reside on any network, anywhere</td>
</tr>
<tr>
<td>• The firewall must be dropped or a long list of exceptions must be allowed</td>
<td>• Allow an exception for one single port in the firewall</td>
</tr>
<tr>
<td>• Security permissions must be configured in Windows</td>
<td>• Optional security settings (certificate exchange and encryption) are handled by the application</td>
</tr>
<tr>
<td>• Authentication handled by Windows LDAP and Username/Password must match</td>
<td>• Optional authentication handled by the application</td>
</tr>
<tr>
<td>• Thus, strong dependency on Windows</td>
<td>• Everything in the app so no OS dependence</td>
</tr>
</tbody>
</table>

- OPC DA and DCOM: DCOM/OPC DA applications typically must reside on the same network. The firewall must be dropped or a long list of exceptions must be allowed. Security permissions must be configured in Windows, and authentication is handled by Windows LDAP. This results in a strong dependency on Windows.

- OPC UA and Binary/TCP: OPC UA and Binary/TCP applications may reside on any network, anywhere. An exception can be set for one single port in the firewall. Optional security settings (certificate exchange and encryption) are handled by the application. Optional authentication is handled by the application, and everything is in the app, so there is no OS dependency.
OPC TUNNELING
WHY THE NEED FOR TUNNELING?
WHY THE NEED FOR TUNNELING?

When applications do not support OPC UA, but a communications path through barriers (such as across networks or firewalls) is needed, users can use an intermediate "tunneling" application. Perhaps to:

• Allow an OPC DA client on one network to talk to a device or an OPC DA server on a different network
• Use an OPC DA client without configuring DCOM settings
• Allow a non-OPC client on one network to talk to a device or OPC DA server on a different network
• Enable a device on one network to exchange data with a device on another network
• Add security to communications
OPC-UA REMOTE COMMUNICATIONS

- Firewall Friendly
  - Based on TCP
  - Certificate exchange or User/Password
  - One single port (configurable)
  - No need for 3rd party tunneling solutions
CONNECTIVITY PLATFORM
INCREASING COMPLEXITY

- Connectivity
- Data quantity, quality, and reliability
- System security
- Usability
- Changing technology
REDUCING COMPLEXITY
DATAFLOW MACRO VIEW
PLATFORM: CENTRALIZED COMMUNICATIONS

- Consolidates data and information from various sources into one communications platform
- Provides consistent and reliable data throughout the enterprise
- Reduces network traffic
- Decreases device and system resource usage
- Reduces training, support, and maintenance
REMOTE OPC-DA CONNECTION

Oil&Gas & Petro Chemical
REMOTE OPC-DA CONNECTION – OIL&GAS & PETROCHEM
REMOTE OPC-DA CONNECTION – OIL&GAS & PETROCHEM
CONNECT IT & OT NETWORKS

Pharma
OPC for Industrial Control Systems

Hector Garcia
Kepware Channel Manager, Europe
hector.garcia@Kepware.com

11/10/2018