Secure & Reliable Communication of Information Using OPC UA

Paul Hunkar
Consultant
DS Interoperability
• **PAUL HUNKAR**
  - President DS Interoperability - Independent Consultant
  - Extensive OPC Knowledge
    - Editor for multiple parts of OPC UA Standard
    - Chairman for OPC UA ISA-95 Working Group
    - Active in multiple collaboration efforts (MDIS, DS-TAS, MTConnect…)
    - OPC Technical Advisory Council Member
  - Over 30 years experience in the Automation Industry
    - Historians, Advanced Controls, New Technology, Operator Consoles
Overview

Three Major sections

- OPC Classic & OPC UA
- Security
- Information vs Data

Summary
Overview

- Summary OPC
- Show small device (demo) – remote connection via phone
- Overview of security / reliability
- (show GDS? Or show security?)
- Overview of information models
- Groups – details
- Vendors (Yokogawa)
- Calculation engine (show app)
- PLC Open – show embedded device again
Consumer Electronics

- Consumer-electronics are driving the way of future with respect to setting the stage for the engineers of today and tomorrow and expectations in industrial automation.

- Engineers expect that they can purchase and use products from multiple vendors and a work out-of-the-box courtesy of consumer-electronics.
Business value proposition

• Total Cost Of Ownership
• Multiple Vendors
• Multiple Products
• Expectations Of Multivendor Interoperability
• Information Integration
• Plug-and-play Not Plug And Pray
• Systems Thinking
• Consumer-electronics Driving Expectations
History: The “original problem”

- Before OPC

<table>
<thead>
<tr>
<th>HMI #A</th>
<th>HMI #B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modbus</td>
<td>Modbus</td>
</tr>
<tr>
<td>Profibus</td>
<td>Profibus</td>
</tr>
<tr>
<td>Profinet</td>
<td>Profinet</td>
</tr>
<tr>
<td>DH+</td>
<td>DH+</td>
</tr>
<tr>
<td>FF</td>
<td>FF</td>
</tr>
<tr>
<td>CIP</td>
<td>CIP</td>
</tr>
<tr>
<td>EGD</td>
<td>EGD</td>
</tr>
<tr>
<td>Bacnet</td>
<td>Bacnet</td>
</tr>
<tr>
<td>DNP</td>
<td>DNP</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP</td>
</tr>
<tr>
<td>TSAA</td>
<td>TSAA</td>
</tr>
<tr>
<td>AS511</td>
<td>AS511</td>
</tr>
<tr>
<td>UDC</td>
<td>UDC</td>
</tr>
<tr>
<td>Others…</td>
<td>Others…</td>
</tr>
</tbody>
</table>

- With OPC

<table>
<thead>
<tr>
<th>HMI #A</th>
<th>HMI #B</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPC</td>
<td>OPC</td>
</tr>
<tr>
<td>Modbus</td>
<td>OPC</td>
</tr>
<tr>
<td>Profinet</td>
<td>OPC</td>
</tr>
<tr>
<td>DH+</td>
<td>OPC</td>
</tr>
<tr>
<td>Bacnet</td>
<td>OPC</td>
</tr>
<tr>
<td>Others</td>
<td>OPC</td>
</tr>
</tbody>
</table>

OPC Server

PLC  DCS  Controller

PLC  DCS  Controller
OPC – De Facto Standard Industrial Automation

- OPC Foundation has more then 470+ members
- 27,000+ products use OPC
- Millions of installations of OPC worldwide
- Most of the deployments use what is now called OPC Classic which is a DCOM based protocol created in the 1990’s.
- OPC eliminated the point-to-point communication problems the industry experienced
  - This reduced cost for end users and system suppliers
  - Eliminated problems with individual drivers being updated
History: Technology evolved...

- More capabilities needed in DA - OPC Data Access 1.0, 2.05a, 3.0
- Need to store real-time values - OPC Historical Data Access
- Need to standardize Alarm Notifications - OPC Alarms & Conditions
- Need to standardize Data Acquisition via internet - OPC XML-DA
- Need to allow PLC-to-PLC communications - OPC Data eXchange
- Need to secure access to servers/tags - OPC Security
- Need to standardize batch-process operations - OPC Batch
- Need to standardize a simple PLC program - OPC Commands
## Features Provided By OPC Classic

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover OPC Servers on the network/ PC</td>
<td>Clients can be completely agnostic to the underlying PLC, protocol, and addressing scheme</td>
</tr>
<tr>
<td>View the tags available in the server</td>
<td>Easy configuration possible by simply pointing + clicking</td>
</tr>
<tr>
<td>Tags could be grouped into a hierarchy</td>
<td>Reading and writing to tags is much easier than memorizing a PLC address</td>
</tr>
<tr>
<td>Read one or more tags</td>
<td>Optimized traffic on the wire thanks to a highly-efficient subscription model.</td>
</tr>
<tr>
<td>Write to one or more tags</td>
<td>• Adding more clients does not necessarily add more overhead.</td>
</tr>
<tr>
<td>Subscribe to tags and receive value-change notifications</td>
<td></td>
</tr>
<tr>
<td>Easily identify good/ bad data</td>
<td></td>
</tr>
</tbody>
</table>
Benefits From OPC Adoption

- Vendors were no longer required to maintain extensive device protocol libraries
- High-quality and affordable device-drivers (Servers) emerged
- More specialized Clients emerged
- Developer toolkits emerged for rapid development of custom applications that could also integrate with the OPC infrastructure
- End-users could mix-and-match numerous vendor products to achieve the best overall solution
Use cases OPC was designed for

- OPC Classic was designed as standard API for HMI / SCADA systems to access process data provided by different protocol drivers
- OPC A&E and HDA were designed as standard API to access alarm and history data managed by SCADA systems
OPC Classic – Limits

- MES and/or HMI Application (OPC Client)
- Windows PC
- DCOM
- OPC Server
- Internet Firewalls
- Embedded HMI
- No Standard
- PLC


- Windows PC
- Tunnel Alternate OS
- PLC

Proprietary Protocol
OPC Data Access
Requirements for OPC UA

Wide adoption of OPC

- Security
  - Access control

- Performance

- Internet
  - Firewalls

Communication between distributed systems

- Robustness
  - Fault tolerant

- Redundancy
  - Fault tolerant

Platform independent

OPC used as common system interface

- SCADA & DCS
- Embedded devices

Scalability

- MES ERP
- Common model for all OPC data

Modeling Data

- Complex data
- Method calls
- Meta information

Base for other standard data models

Type system

- Meta information

Requirements for OPC UA
Use cases OPC UA was designed for

OPC UA was design to include:

- Embedded devices direct to higher levels
- Communication between embedded devices
- Remote sensors
- Direct Integration at the enterprise level
Unified Data

• Existing OPC Classic DCOM interfaces:
  – Each passes a specific type of data
  – No relationship of data between interfaces
  – Relating data is done by the client

• Unified Architecture (UA) interfaces:
  – Single set of Services
  – Information models relate data
    • Example:
      For one tag like TI-101, the current process value, alarm messages, and historical values can be obtained in one request to the server.
    • In OPC Classic the client program would need to make three requests to three different servers

![Diagram of OPC Classic vs. OPC Unified Architecture]
Unified Data: Information Models

- OPC UA modeling language allows custom information models
- Extensible & built on the standard base services
- Many other organizations have built information models on top of it
Development Environment Independence

• No Microsoft, or other IT supplier, technology required
  – Operating system independent
  – Programming language independent

• Clients and servers are running on:
  – Windows 7 and 8, Linux,
    VxWorks, Embedded OS’s, ….

• UA clients and servers have been written in different programming languages:
  – C# (.Net), C++, C, Java, …

• Benefit to end users:
  – More options for client and servers to run in the environment of your choosing
  – Longer lived technology since it is not tied to any one product family
OPC UA: Available Platforms

- Microchip
- Desktop PC
- Smartphone
- PLC/Controller
- Laptop
- Tablet
- Enterprise Servers

OPC UA
Protocol Independence

- Transport protocol and application data layers are separated.
- Different transports can be used with no change to the data configuration.
- Transport choices:
  - Web Services:
    - Uses IT standards such as WS Security and WS Secure Conversation.
  - UA Native Binary:
    - Optimized for high speed data transfer.
- Choices an integral part of the OPC UA specifications.
Communication Layering

- Abstract UA Model Specification
- Business Model, Abstract Service Definition
- Scalable Platform Independent Messaging Model
- .NET (WCF) Version
  Portable C/C++ Version
  Java Version
- WSDL / SOAP or TCP / Binary Services Binding
- Proxy / Stubs
- API

Tool or Language Dependent (e.g. .NET)
Unified Data: Specification Layering

- Clients written to just the base can access all data from the higher level layers
- OPC Foundation information models cover most OPC Classic functions
- Industry, company or system specific information models can be added without changing the base services
Robust

- Features added based upon years of experience with OPC Classic

  - Subscription Update Features
    - Keep-alive (heartbeat) messages
      - Allows clients to detect a failed server or channel
    - Sequence Numbers in each update message
      - Allows client re-sync to obtain missed messages

- Redundancy
  - Built into the base services
  - Designed for easy (optional) redundancy of both Clients and Servers

Reliability by design
Backward Compatible

- Existing OPC Classic clients and servers can be used with OPC UA clients and servers using wrappers.

- A wrapper talks OPC Classic and OPC UA protocols.
Forward Looking

- Firewall Friendly
- Relay and cloud based computing
OPC UA Scalability & Profiles

Functionality needed varies according to system
Security

- Application Security
- User Level security
- Message Security
- Audit mechanisms

All selectable by End User
Timeline

Version 1.0
Internal Release
Modeling Language
Services
Base Model

Version 1.1
Public Release
Protocols
Built-in Models
- Data access
- Alarms & Conditions
- Programs

2007
Draft
Protocols
Built-in Models

2008
Draft

2009
Version 1.1

2010
Version 1.2
Maintenance Release
Historical Access
Compliance Updates
New features
- HTTPs Protocol
- File transfer

2011

2012

2013

2014

Version 1.3
Maintenance Release
Network Discovery
Central PKI
New Features
- Durable Queues
- Union Data Types
- Bit Mask Data Type

Draft
Network Discovery

UA Products Available
OPC Foundation Domains

The key markets for OPC technology include:

- Industrial Automation
- Building Automation
- Embedded Devices
- Energy Management (Smart Grid)
- Manufacturing Enterprise Management
- M2M
- Cloud-based Computing
OPC UA Key Features

• Unified Data
• Platform Independence
• Protocol Independence
• Robust
• Security
• Performance
• Backwards Compatible
Demo

- Raspberry PI
  - 512 MB
  - Arm Processor
  - Unified Automation SDK
  - Full sample server

- Smartphone
  - UA expert sample client
Questions

- **Paul Hunkar**
- Technical Director
- [Paul.Hunkar@DSIInteroperability.com](mailto:Paul.Hunkar@DSIInteroperability.com)