OPC Unified Architecture (OPC UA) and the DeltaV system

OPC UA is a platform-independent standard that enables secure communication between control systems, devices, and enterprise software. It is especially suited to manufacturing and process control applications.

Communication works on a clients/server model. Each client can interact concurrently with one or more servers. Each server can interact concurrently with one or more clients.

OPC UA server data is stored in an address space. Each entity in the address space is a node. Servers provide clients with type definitions to enable the clients to read the address space structure. Clients typically provide a user interface that enables users to identify the specific node variables that they want the client to read or write to. Address spaces can contain real-time data, alarms and events, and history.

DeltaV systems provide extensive support for OPC UA. DeltaV software:

- Enables third-party OPC UA clients to read DeltaV real-time, historic, and alarm and event data.
- Enables DeltaV OPC UA clients to read data from third-party devices, systems and software. Typically, a DeltaV OPC UA client reads data from a third-party OPC UA server and writes the data to a DeltaV module.

OPC UA security is based on digital certificates. The security model includes encryption, authentication and auditing to ensure that data going into your system is authenticated and data going out is secure.

You can configure the following DeltaV nodes as OPC UA servers:

- ProfessionalPLUS workstation
- Application workstation
- PK controller

You can configure the following nodes as DeltaV OPC UA clients:

- ProfessionalPLUS workstation
- Application workstation
- Ethernet I/O card (EIOC)

An OPC UA activation license is required for OPC UA servers and clients in workstations. This is a one-time and system wide license that activates all the OPC UA servers and clients in all the Application stations and ProfessionalPLUS workstations in the system. Once the OPC UA activation license is present, the OPC UA server consumes licenses from classic OPC servers (DA, A&E and HDA). These licenses will be shared with OPC Classic and OPC UA clients. For example: If you have an application station with a 10000 OPC DA Classic license, you can have one OPC UA client and one OPC DA client each consuming 5,000 signals.

Note: OPC UA workstation clients and servers are for monitoring and non-critical control. The system does not set overall module integrity (OINTEG) to BAD due to module slippage.

Note: All OPC UA clients and servers in your OPC UA application require a common time source to remain functional. You can use NTP or an equivalent. This includes DeltaV clients and servers and third-party clients and servers regardless of platform type or operating system.

DeltaV OPC UA application examples

Here are some typical applications of DeltaV OPC UA servers and clients:

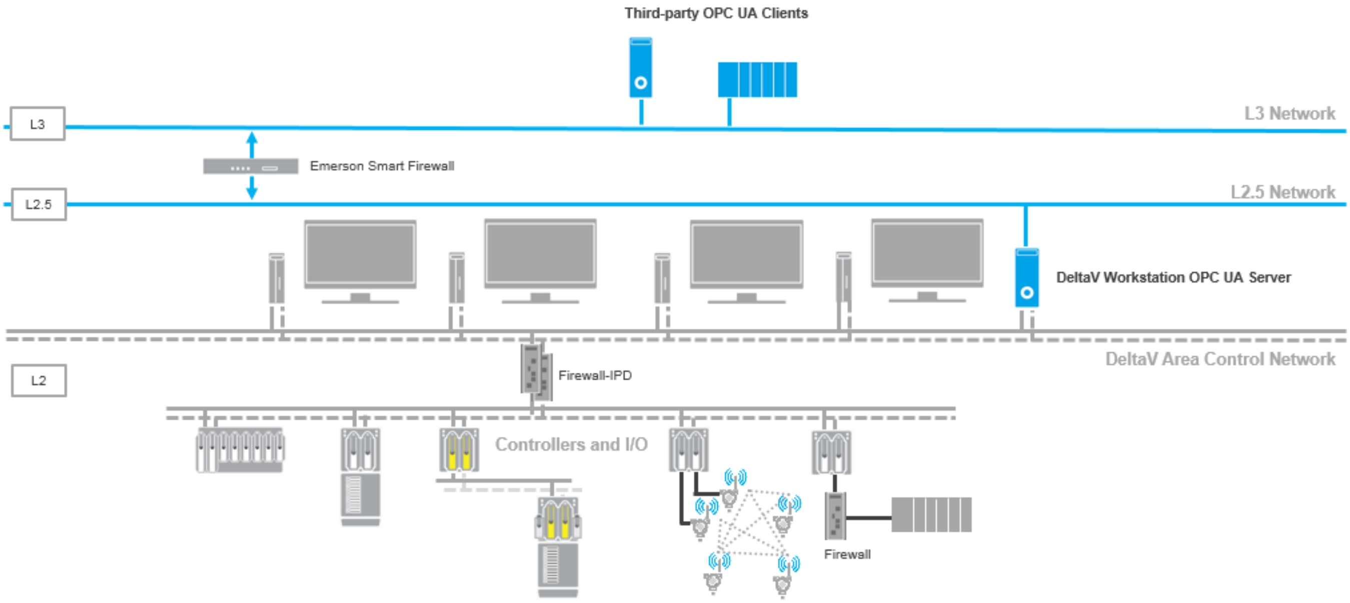
- OPC UA server in the PK controller serves real-time module data to an OPC UA client, typically third-party historian or a local HMI panel.
- Workstation OPC UA server provides real-time data, historical data and alarms event data to any OPC client that consumes that information. Typical examples include enterprise historians and any MES layer applications. It basically replaces OPC Classic servers.
- EIOC OPC UA client reads and writes from a third-party OPC UA servers. The servers can be on the MES layer or on a plant LAN (for example, PLCs).
- Workstation OPC UA client reads and writes real-time data from a third-party OPC UA server. Typically, this is used to replace OPC Mirror applications that connect to servers in the MES layer.

DeltaV OPC UA network examples

The following diagrams are examples of typical networks that include DeltaV OPC UA clients and servers and third-party OPC UA clients and servers.

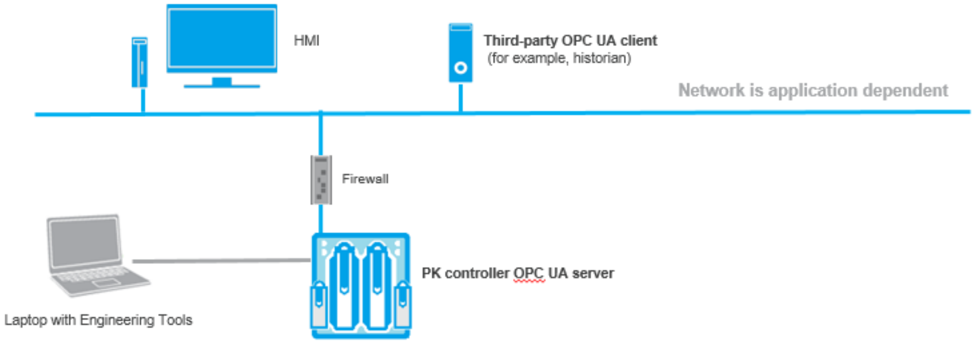
DeltaV ProfessionalPLUS workstations and application workstations can be configured as OPC UA servers and connect to third-party OPC UA clients. Refer to the diagram for a typical installation.

DeltaV workstation OPC UA server and third-party clients



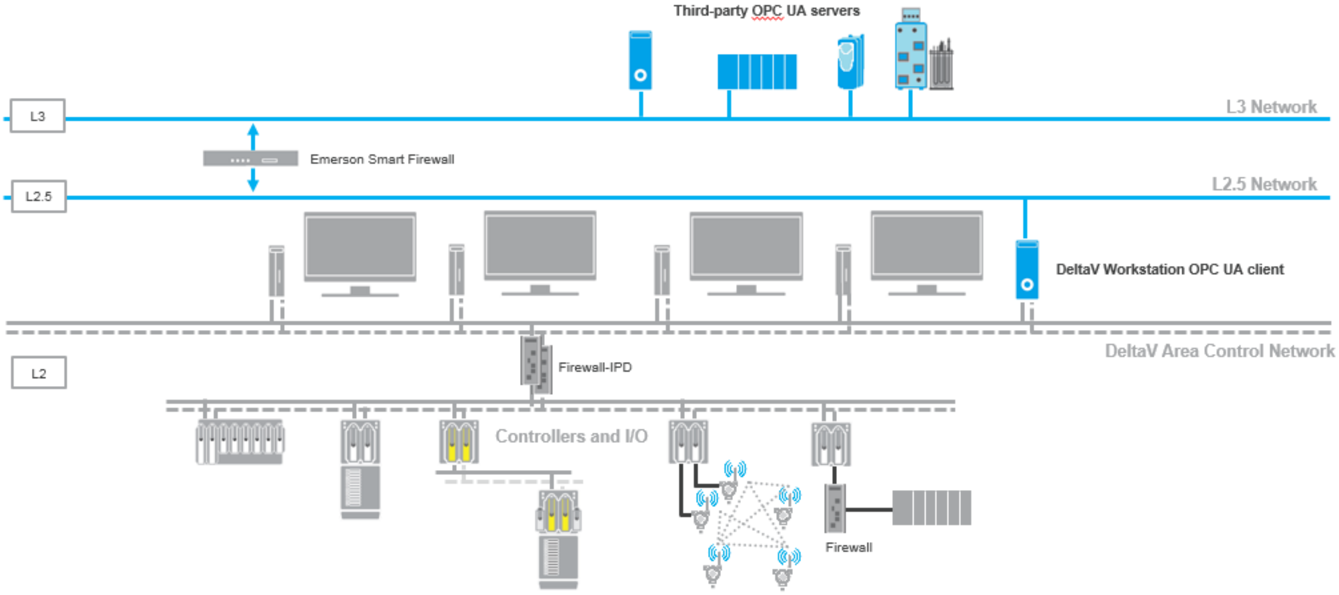
DeltaV PK controllers can be configured as OPC UA servers and connect to third-party OPC UA clients. Refer to the diagram for a typical installation.

DeltaV PK controller OPC UA server and third-party client


HMI
Third-party OPC UA client
(for example, historian)
Network is application dependent
Firewall
PK controller OPC UA server
Laptop with Engineering Tools

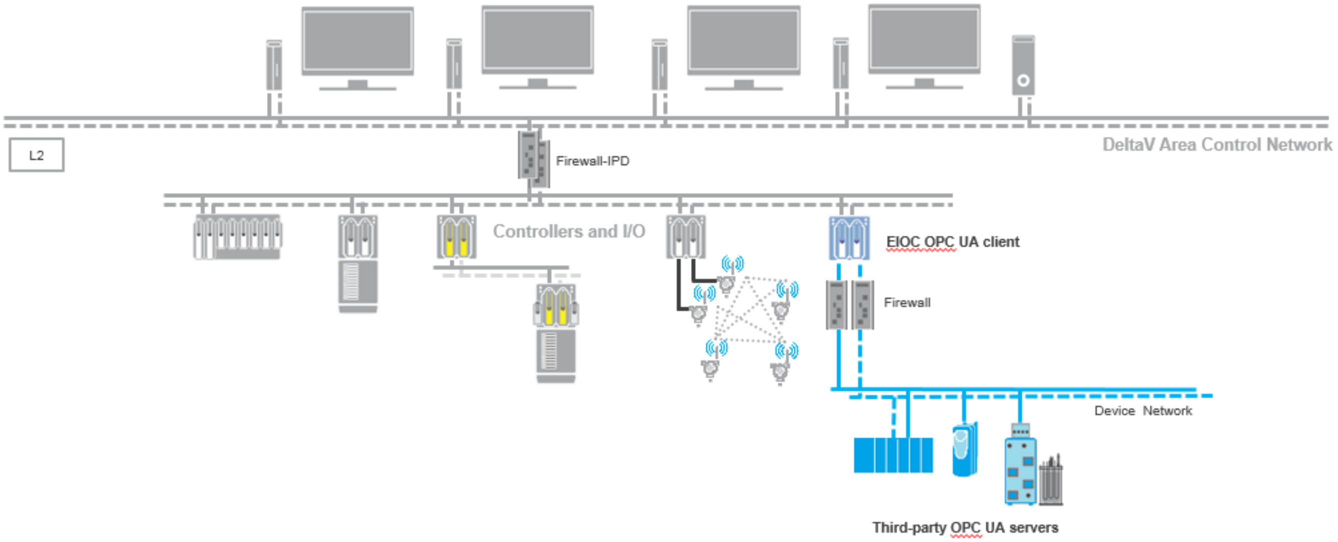
DeltaV ProfessionalPLUS workstations and applications stations can be configured as OPC UA clients and connect to third-party OPC UA servers. Refer to the diagram for an example installation with third-party servers on the level 3 network.

DeltaV workstation OPC UA client and third-party servers



DeltaV Ethernet I/O cards can be configured as OPC UA clients and connect to third-party OPC UA servers. Refer to the diagram for an example installation with third-party servers on the device network.

DeltaV EIOC OPC UA client and third-party servers



DeltaV OPC UA servers

The table shows the types of data that DeltaV OPC UA servers can share with OPC UA clients.

DeltaV node type	Real-time module data	Historical data	Alarms and Events
ProfessionalPLUS and Application workstations	Yes	Yes	Yes
PK controller	Yes	No	No

DeltaV OPC UA servers store data in an OPC UA-compliant address space. The DeltaV system populates the address space automatically. For example, the workstation address spaces contain:

- Alarms and Events for the areas assigned to the workstation
- Module data for modules in the areas assigned to the workstation
- Continuous Historical data that is enabled for this workstation

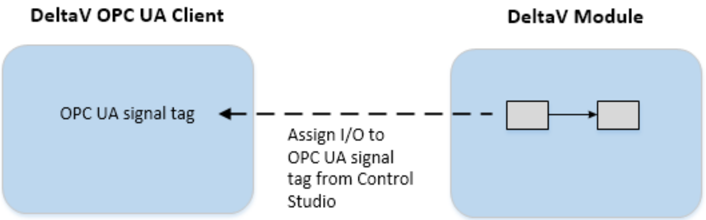
- Workstation diagnostic parameters
- OPC UA-specific parameters

Note: DeltaV OPC UA servers do not support off-line nodesets.

DeltaV OPC UA clients

DeltaV OPC clients contain the following subsystems:

- **OPC UA Physical Devices (PDTs):** establish the communication link to a single OPC UA server through the server's endpoint URL. The physical device stores the configuration information for a connection to an OPC UA server. Each physical device is typically configured to communicate with one server. In redundant network configurations, you can configure a secondary UA server as well.
- **OPC UA Logical Devices:** group related signals using common settings and define the interval at which the client gets data from the server.
- **OPC UA Signals:** map the client to an OPC UA variable node in the server address space. To use the server data in the DeltaV system, you need to assign function block parameters to the OPC UA signals. OPC UA signals include a signal tag. You assign a block parameter to an OPC UA signal tag using the **Assign I/O > To Signal Tag** command in Control Studio.



EIOC OPC UA client signal tags can only be assigned to function block and module parameters assigned to that EIOC. These parameters can also be referenced by other controllers or workstations. You can also use the signal through external and internal references or blocks that support expressions (for example, the CALC and Action blocks).

Workstation OPC UA client signal tags can only be assigned to function block and module parameters assigned to that workstation. These parameters can also be referenced by other controllers or workstations.

Note: Performing a partial download on any of the following items disconnects and reconnects the session even if no changes have been made:

- OPC UA physical device (PDT)
- EIOC port using the OPC UA protocol
- Workstation OPC UA Client subsystem

DeltaV OPC UA supported data types

The table shows the OPC UA data types supported by DeltaV OPC UA.

Supported OPC UA data types

Supported data type	Notes
Boolean	0=FALSE, 1=TRUE DeltaV OPC UA treats Boolean data types as Int32 parameters where all values are resolved to either 1 or 0 rather than True or False.
Sbyte Byte Int16 Unit16 Int32 UInt32 Float	8-bit signed integer, 16-bit signed integer, and 32-bit signed integer are treated as Int32 data types: 8-bit unsigned integer, 16-bit unsigned integer, 32-bit unsigned integer, and 32-bit unsigned integer with status are treated as UInt32 data types. 64-bit is not supported. This includes Double, Int64, UInt64, and TimeStamp. Float values follow the IEEE 754-1985 Standard. A Float value can have any numeric data type.
String	DeltaV OPC UA allows the reading of strings. Writing strings is not supported. EIOC and workstation OPC UA clients support a maximum of 10 string signal inputs (reads) per LDT.

DeltaV OPC UA server and client capacities

DeltaV OPC UA Server Capacity

Description	Application Station	Profes
Real-Time Data (DA)	30,000 monitored items per second c_opc_ua_specifications.html#r_opc_ua_capacities__fn_0 (https://guardian.emerson.com/docs/DELTAV/BOL/bol1431/c_opc_ua_specifications.html#r_opc_ua_capacities__fn_0) 2,000 writes per second 100 concurrent clients	250 mo (https:/ 2 concu
Alarms and Events (A&E)	300 events per second 25 concurrent clients	300 eve (https:/ 25 conc
Historical Data (HDA)	7,000 parameters per second 25 concurrent clients	7,000 p (https:/ 25 conc
Transportation	Binary, HTTP, and HTTPS	Binary,
Redundancy	Not supported	Not sup

DeltaV OPC UA Client Capacity

Description	Application Station	Pr
Real-Time Data (DA)	30,000 monitored items per second 15,000 writes per second 64 concurrent clients c_opc_ua_specifications.html#r_opc_ua_capacities__fn_clients (https://guardian.emerson.com/docs/DELTAV/BOL/bol1431/c_opc_ua_specifications.html#r_opc_ua_capacities__fn_clients)	30 (h 15 (h 64 (h
Alarms and Events (A&E)	Not supported	No
Historical Data (HDA)	Not supported	No
Transportation	Binary	Bi
Redundancy	No	No

Notes on OPC UA capacities

- All performance specifications provided are with OPC UA security disabled in the clients and servers and have a ±3% variation. Expect lesser communications performance if security is enabled.
- Workstation-based control using OPC UA clients or servers does not provide the same performance as physical controllers or EIOCs but is acceptable for most monitoring and non-critical control applications. Specifically, workstation-based control is supported for a minimum of 1 second execution (compared to 100 milliseconds in a physical controller).

[1] Client redundancy might affect the number of items that are used. For example, a redundant EIOC OPC UA client uses twice the number of configured items.

[2] The PK controller supports six concurrent sessions that can be consumed by three clients. A redundant OPC UA client connected to the PK controller consumes more than one session.

[3] HDA and A&E performance in the ProfessionalPlus may be less due the number of critical applications running in the workstation. If you have specific performance requirements for HDA and A&E applications, use a dedicated Applications Station.

[4] High Availability means that when a controller switchover occurs, the client will be disconnected. The OPC UA server is available to the new active controller almost immediately, using the same IP address but a different MAC address. The client is responsible for re-connecting with the OPC UA server once the server is active.

[5] When connecting a PK controller to a redundant OPC UA client with redundant communications (for example, an EIOC), the client can consume four times the monitored items and four times the number of sessions from the OPC UA server. In this scenario, the maximum capacity is 1,250 monitored items/sec and four sessions (leaving two sessions for diagnostics).

[6] Clients are equivalent to Physical Devices (PDTs) when configuring the OPC UA clients in DeltaV Explorer.

[7] The performance of the ProfessionalPLUS OPC UA client may be less due the number of critical applications that run in the workstation. If you have specific communications performance requirements the OPC UA client, use a dedicated Applications Station or an EIOC.

[8] (https://guardian.emerson.com/docs/DELTAV/BOL/bol1431/#fnsrc_8) Redundant installations use more sessions and tags. For example, a redundant EIOC on a single device network consumes two sessions and twice the amount of tags from the OPC UA server to which it is connected. A non-redundant EIOC on a redundant device network also consumes two sessions and twice the amount of tags. A redundant EIOC on a redundant device network consumes four sessions and four times the amount of tags.

DeltaV OPC UA redundancy support

DeltaV OPC UA supports redundancy as follows:

- DeltaV OPC UA clients support transparent redundancy server failover.
- DeltaV OPC UA clients support non-transparent redundancy with the following failover methods: None, Cold, and Warm.
- DeltaV PK controller can be redundant, but the PK controller OPC UA server does not support transparent or non-transparent failover.
- DeltaV OPC UA workstation servers do not support redundancy.

Create an OPC UA server

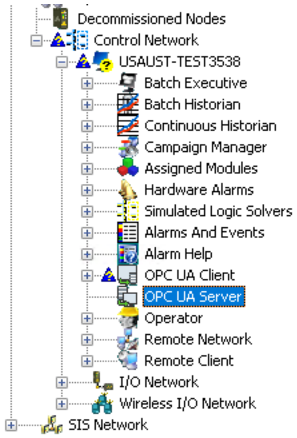
About this task

Note: This task describes how to create a DeltaV OPC UA server without security features. Refer to the related information for information on OPC UA security.

Procedure

1. Navigate to the OPC UA Server subsystem in the DeltaV Explorer hierarchy. The OPC UA server subsystem is underProfessionalPlus workstations, Application workstations, and DeltaV PK controllers. This procedure is for an OPC UA server on a ProfessionalPlus workstation. Creating a server on a DeltaV PK controller is similar.

   Note: Make sure the node name does not contain a **$** character. This is not a legal character in OPC UA applications with digital certificates.

2. Select the **OPC UA Server** subsystem, right-click and select **Properties**. The system displays the **OPC UA Server** dialog.
3. Click **Enable OPC UA Server**.
   Important:
   Enabling the OPC UA server can consume large amounts of memory (viewable in the FreMem parameter). This happens because OPC UA creates an address space for every parameter of every function block in each module in the controller.
4. On the **General** tab, select an option under **User Authentication**. Refer to Related information for topics on security and user authentication.
5. Use the **Certificate** tab to generate or import your certificate.

6. The PK controller's OPC UA server has an **Advanced** tab. Use this to specify the primary and secondary port addresses.
   The endpoint URL is shown on the **Advanced** tab.
7. Click **OK**.
8. Right-click the **OPC UA Server** and select **Download**.

Change the OPC UA server's port

About this task

You can modify the default port on the workstation OPC UA server using this procedure.

Procedure

1. From DeltaV Explorer, select the OPC UA server node.
2. Right click and select **Properties** from the context menu.
3. Select the OPC UA Server subsystem. In the right pane, select the endpoint URL. Right click and select **Properties**.
4. Edit the port number in the **Port** field.

   Note:
   This changes the **Endpoint Url** field after downloading.
5. Click **OK** to save the change.
6. Download the OPC UA server. To copy the new endpoint URL for your OPC UA clients, go back to the endpoint's **Properties** dialog.
7. For workstation servers using HTTPS endpoint URL, get the following information about the existing bound certificate using the netsh command.
   - Certificate Hash
   - Application ID

   a. From the Start menu, open a command prompt.
   b. Type `netsh http show sslcert ipport=0.0.0.0:[PORT]` and press Enter. The port is 9408 by default.
   c. Highlight the number needed and press `Ctrl C` to copy it.
   d. In a text editor, paste the number (label it for use later).
   e. Repeat for the other number.
8. For workstation servers using HTTPS endpoint URL, delete the existing certificate binding (the old port): `netsh http delete sslcert ipport=0.0.0.0:[PORT]` The port is 9408 by default.
9. For workstation servers using HTTPS endpoint URL, bind the certificate to the new port: `netsh http add sslcert ipport=0.0.0.0:[PORT] certhash=[CERTHASH] certstorename=Root appid=[APPGUID]`
   When using a self-signed certificate, the `certstorename` parameter is set to `my`.
10. For workstation servers using HTTPS endpoint URL, verify that the SSL certificate has been bound to the new port: `netsh http show sslcert ipport=0.0.0.0:[PORT]`

    The software displays the SSL certificate bindings.
11. Open the new port on any firewalls (including Windows firewalls) between the OPC UA server and its clients for all protocols that you are using (HTTP, HTTPS, OPC.TCP).

Create a DeltaV OPC UA client

Before you begin

- To create a working client, you need to know the endpoint URL of the associated OPC UA server. Record the server's opc.tcp protocol URL before creating a client. To obtain the url of a DeltaV server:
  - For DeltaV workstation servers, click the OPC UA Server subsystem in the left pane of DeltaV Explorer. The right pane displays the opc.tcp endpoint url. Right click the endpoint and click **Properties**. Copy the url from the dialog.
  - For DeltaV PK controller servers, click the OPC UA Server subsystem in the left pane of DeltaV Explorer and right-click **Properties**. Click the **Advanced** tab and copy the endpoint url.

  Note:
  The endpoint URL is not contained in the OPC UA server's FHX file. To reconstruct the URL, you can use the node's information in this format: *protocol://machine:port/path*. For example, *opc.tcp://192.168.1.2:4880/DVOpcUaServer* (where *192.168.1.2* is the node's IP address. For workstation-based OPC UA servers, the hostname (the node's computer name) is valid in place of the IP address).
- For EIOC clients, the port protocol must be **OPC UA**. To set the protocol, open the EIOC port properties in DeltaV Explorer, click the **Advanced** tab and select **OPC UA** under the **Protocol** drop-down list.

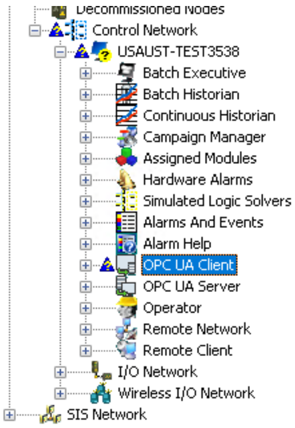
About this task

Note: This task describes how to create a DeltaV OPC UA client without security features. Refer to the related information for information on OPC UA security.

Procedure

1. Navigate to the **OPC UA Client** subsystem in the DeltaV Explorer hierarchy. The client is under ProfessionalPlus workstations, Application workstations and EIOCs. This procedure is for a client on the ProfessionalPlus. The procedure for other client types is similar.

   Note: Make sure the node name does not contain a **$** character. This is not a legal character in OPC UA applications with digital certificates.

   - Decommissioned Nodes
   - Control Network
     - USAUST-TEST3538
       - Batch Executive
       - Batch Historian
       - Continuous Historian
       - Campaign Manager
       - Assigned Modules
       - Hardware Alarms
       - Simulated Logic Solvers
       - Alarms And Events
       - Alarm Help
       - OPC UA Client
       - OPC UA Server
       - Operator
       - Remote Network
       - Remote Client
     - I/O Network
     - Wireless I/O Network
   - SIS Network

2. Select the OPC UA Client and right-click **Properties**. The system displays the **OPC UA Client** dialog.
3. Click **Enable OPC UA Client**.
4. Click the **Certificate** tab.
5. Click **OK**.
6. Select the OPC UA Client and right-click, **New OPC UA Physical Device**. The system displays the physical device (PDT) properties dialog.
7. On the **General** tab, enter a description for the physical device. Physical devices correspond to OPC UA servers. You may want to include information in the description that identifies the server.
8. On the **Primary** tab, enter the opc.tpc protocol URL for the server in the **Endpoint Url** field.

   Note:
   If the URL contains a hostname and not an IP address, you must have a DNS server configured that will resolve that hostname to a static IP address with a lease time set to infinite (so that the IP address will remain in the DNS table). If a dynamic IP address is used for your endpoint (such as one assigned by DHCP), you will have to update the DNS table with the new IP address every time it is reassigned.

9. For redundant servers, enter the secondary opc.tcp protocol URL on the **Secondary** tab. This step is not required for simplex servers.
10. Click **OK**.
11. Select the physical device in the DeltaV Explorer hierarchy and right-click, **New OPC UA Logical Device**. The system names physical devices PDT1, PDT2, and so on.
12. Select the logical device and right-click **Properties**. The software displays the **OPC UA Logical Device** dialog. The system names logical devices LDT1, LDT2, and so on.
13. On the **General** tab, enter a description to differentiate this from other logical devices.
14. On the **Subscription Settings** tab, enter the **Publishing Interval**. The publishing interval is the interval at which the client pulls data from the server.
15. Click **OK**.
16. Click the **OPC UA Client**, then right-click **Download**.

    The system displays the **Confirm Partial Download** dialog.
17. Click **Yes**.
18. If you receive any warnings (for example, the primary connection for PDT1 does not have a server application certificate configured), click **Download Anyway**.
19. Before creating signals in the client to read server data, test to make sure that the client can communication with the server.

DNS and EIOC as an OPC UA client

A DNS server is only necessary when a hostname is configured instead of an IP address as the endpoint URL on the client (the URL to the OPC UA server). As a result, DNS lookup is only enabled on the EIOC when a hostname is configured.

The EIOC supports redundant DNS servers. The calculated address is the x.x.x.1 address of the subnet and it is calculated specifically for the primary and secondary device network IP addresses. The DNS is disabled if the EIOC is configured at the x.x.x.1 address; but, this is handled independently on the primary and secondary networks (meaning that the DNS can be selectively disabled on each network). Also, a disabled network (configured as all zeros) does not have a defined DNS address.

Though it is possible to configure the primary and secondary networks using hostnames, care needs to be taken to ensure the hostnames resolve to appropriate addresses for each subnet. If the same hostname is used for both networks or if two different hostnames resolve to the same IP, all communications will be in the same subnet and therefore be sent over the same network. An improperly configured redundant setup does not actually communicate redundantly.

If redundant DNS servers are configured, it is assumed that both servers are identical. This requires both DNS servers be able to resolve all hostnames for both the primary and secondary networks. The EIOC will attempt to resolve all hostnames through the primary DNS, only contacting the secondary DNS if the connection to the primary fails. If the primary responds with *unknown address*, the EIOC will not contact the secondary as it expects the same response.

It is possible to configure two network paths to the same DNS server, though that configuration does not provide DNS node redundancy.

If the hostname resolves to an address outside of the configured subnets, the EIOC will attempt to reach the node through the default gateway on the primary network.

IPv4 Default Gateway for EIOC

The IPv4 default gateway address for the EIOC is set to the x.x.x.1 IP address of the primary device network's subnet for that EIOC. This means the x.x.x.1 IP address is reserved for the default gateway address. If the primary device network is using the x.x.x.1 address, then the default gateway is disabled. Also, a disabled network (configured as all zeros) does not have a defined default gateway address.

Redundant IPv4 default gateways are not provided; therefore, the secondary device network does not have a default IPv4 gateway address.

DNS and IPv4 default gateway on the PK controller with OPC UA

A DNS server is only necessary when configuring an OPC UA client and using a hostname instead of an IP address as the endpoint URL on the client (the URL to the OPC UA server).

Since the OPC UA client is not supported on the PK controller, DNS is not needed and therefore not supported on the PK controller. Also, because the OPC UA server on the PK controller only responds to incoming requests, it does not resolve hostnames and therefore does not require DNS.

IPv4 Default Gateway for the PK controller

The IPv4 default gateway address for the PK controller is set to the x.x.x.1 IP address of the PO1's primary device network's subnet for that particular controller. This means the x.x.x.1 IP address is reserved for the default gateway address. If the PO1's primary device network is using the x.x.x.1 address, then the default gateway is disabled. Also, a disabled network (configured as all zeros) does not have a defined default gateway address.

Redundant IPv4 default gateways are not provided; therefore, the secondary device network does not have a default IPv4 gateway address.

Test OPC UA client-side communications

Procedure

1. From the DeltaV Explorer hierarchy, select the **OPC UA Client**.
2. Right-click **Diagnose**. The software launches DeltaV Diagnostics.
3. From the DeltaV Diagnostics hierarchy, select the physical device (PDT) of the OPC UA Client.
4. Right-click **Test Endpoint Connection**. If successful, the software displays a message indicating that the OPC UA server connection is established.

Troubleshooting communications between OPC UA clients and servers

If the software displays `Unable to connect to OPC UA Server` when you attempt an endpoint connection, check the following to troubleshoot the connection between your client and server.

DeltaV OPC UA clients

- Make sure the OPC UA client is enabled (**OPC UA Client** properties dialog, **General** tab).
- Make sure you have generated a certificate for the client even if you are not implementing security (**OPC UA Client** properties dialog, **Certificates** tab)
- Make sure the server endpoint URL is correct (physical device properties dialog, **Primary** and **Secondary** tabs).
- Make sure the DeltaV OPC UA Server service is running on the host device.

- Make sure the OPC UA client has been downloaded.
- Use the Test Endpoint Connection command in DeltaV Diagnostics to check OPC UA client-side communications.
- If you are implementing security, verify that the security settings on the client and server match. This includes the security policy (None, Basic256Sha256, and so on) and the security mode (None, sign or sign and encrypt).
- If the client fails to connect to a server because a certificate is not trusted or if a logon attempt fails, the client will not try to reconnect. You must download the client physical device to initiate a reconnect attempt. If anonymous authentication is used, no download is required.

DeltaV OPC UA servers

- Make sure the OPC UA server is enabled (**OPC UA Server** properties dialog, **General** tab).
- Make sure you have generated a certificate for the server even if you are not implementing security (**OPC UA Server** properties dialog, **Certificates** tab).
- Verify that an OPC UA session (or sessions) has been created under the OPC UA server in DeltaV Diagnostics.
- On the PK controller, check the status of the server and endpoints in DeltaV Diagnostics.
- Make sure the network allows communication between the OPC UA client and the OPC UA server.
- Make sure the OPC UA server has been downloaded.
- Make sure the DeltaV OPC UA Server service is running.
- Check the server log for a workstation server. To find the location of the server log:
    1. Right-click the OPC UA server and click **Properties**.
    2. Click the **Log Settings** tab.
    3. Note the path in the **Location** field.

Note: OPC UA server communication with one OPC UA client can adversely impact communication with other OPC UA clients. For example, browsing large configurations in some third-party OPC UA clients can impact communication with other clients.

Create OPC UA client signals

About this task

Each OPC UA client signal reads a specific node ID in the OPC UA server.

Procedure

1. In the DeltaV Explorer hierarchy, select the logical device and right-click New OPC UA Signal.
2. The system displays the OPC UA Signal dialog.
3. Click **Browse Online** next to the **Node Id** field. If you have established communication with the server, the system displays the Browse Nodes window. The window enables you to navigate the server’s address space. Items available to the client have a checkbox.

   Note: If your server supports off-line nodesets, the software enables you to browse offline as well. To use an off-line nodeset, click the Browse Offline checkbox and browse to the xml nodeset file through the Windows Explorer.
4. Select the checkbox next to the item you want this signal to read.

   Note: The signal and node ID relationship is one-to-one. You can only select one checkbox per signal.
5. Click **OK**.
6. Click the physical device then right-click **Download > OPC UA Physical Device**.

   Note: If the OPC UA signal is mapped to a dynamic reference parameter, the signal returns the data type of the parameter to which the dynamic reference parameter is bound. For example, if the dynamic reference parameter is bound to a floating point parameter, the OPC UA signal returns a floating point data type. If the bound parameter is changed to another type, the signal goes bad because there is a mismatch. You must manually change the data type of the signal and download the OPC UA client to restore communications.

Assign an OPC UA signal to a function block parameter

About this task

The procedure requires a control module with one or more function blocks that support the assign I/O feature. You can assign function block parameters to OPC UA signals. The module you use must be assigned to the client (either an EIOC or a workstation).

Procedure

1. Navigate to the function block in DeltaV Explorer (for example, **DeltaV System > Control Strategies > Area**).
2. Right-click the function block and then click **Assign I/O > To Signal Tag**.

3. The software displays the I/O properties dialog.
4. Click **Browse** to find a OPC UA signal tag. The software displays the **Browse** dialog.
5. Select a parameter.
6. Make sure the module is assigned to the workstation or EIOC that hosts the OPC UA client.
7. Download the OPC UA client host.