OMRON

OPC UA

User Manual

O086-E-01

OPC UA Interface on Power PMAC

Power PMAC can act as a server on an OPC UA (Open Platform Communications Unified Architecture) client/server network. OPC UA is a popular communications protocol for the Industrial Internet of Things (IIoT) in many factory automation applications.

Power PMAC has the ability to transfer numerous variable values in both directions over the network. The OPC UA interface runs as a separate application on the Power PMAC, communicating to the Power PMAC firmware on one side, and the OPC UA clients over Ethernet on the other.

Requirements

The following conditions are necessary to use Power PMAC's OPC UA Server:

- The Power PMAC must have an ARM CPU (dual-core LS102*x*A or quad-core LS104*x*A). This is available in several form factors, including the CK3E, CK3M, CK5M, UMAC dual-core, UMAC quad-core, Power Brick, and EtherLite).
- The Linux operating system must be from the Debian 12 installation or newer. This was installed at the factory for firmware versions V2.8.0 and newer.
- The Power PMAC firmware must be V2.8.1 or newer.
- For interactive setup of the Server using the IDE, V4.6.4 or newer of the IDE is required.
- Any client computer communicating with the Power PMAC with OPC UA must have an OPC UA client application. One suggested application is the free B Prosys OPC UA browser, available for multiple targets, including Windows PCs, Linux PCs, and mobile devices.

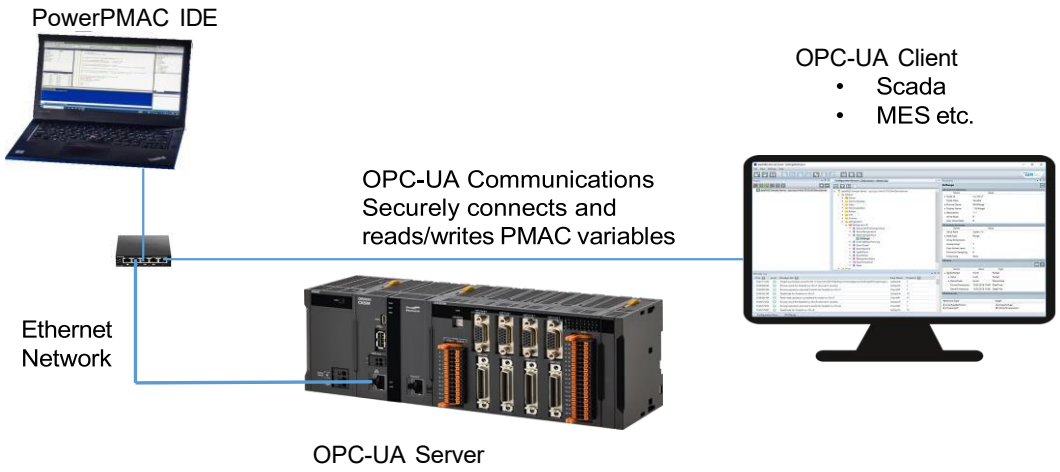
Overview

The OPC UA Server function permits the Power PMAC controller to operate as a server on an OPC UA network. With this function, OPC UA clients can connect to the Power PMAC controller via Ethernet using the standard Ethernet communications port on the Power PMAC CPU. This permits the Power PMAC to send and receive variable values over the OPC UA network with one or more clients.

This OPC UA implementation supports both device authentication and encrypted communication, although neither is required. These features enable secure data exchanges between the Power PMAC and client devices, facilitating SCADA and MES systems, among others, so that host systems can collect manufacturing progress information or issue manufacturing instructions.

System Configuration

Power PMAC's OPC UA Server function supports the following system configuration:



The Windows PC executing the Power PMAC IDE to configure Power PMAC as an OPC UA server can also be a client on the network, but this is not required.

Multiple client devices can be supported on a single Power PMAC OPC UA network.

OPC UA Features

OPC UA communications has the following features:

- It is a versatile global standard network for both discrete control and process control, from the sensor or controller level to the host-monitoring and management level.
- It is defined as a recommended communications standard of "Industry 4.0" to connect OT control networks in factories to IT networks.
- It allows full-scale secure information exchange in an industrial network consisting of differing types of devices.
- It allows the expansion of visualization of information adapting to the system in the object-based address space.

The Power PMAC OPC UA Server function has the following features:

- It allows the controller to connect directly to an OPC UA client over the same Ethernet network used for host communications.
- It makes it easy to transfer information between Power PMAC's low-level EtherCAT control network with its sensor and actuator information and a higher-level network with the OPC UA protocol.

- It permits monitoring of the operational results of the OPC UA Server function using the IDE's OPC log page.

Specifications

Power PMAC's OPC UA Server has the following specifications:

Item		
Connection ports		OPC UA Server can be used simultaneously standard with PMAC Ethernet communications
OPC UA Function		Server function
Transport and data encoding		UA TCP binary
Supported profile and mode		Micro Embedded Device Server Profile
Default endpoint URL (Server URL)		opc.tcp://192.168.0.200:4840/ (default)
Maximum Number of Client Sessions		10
Maximum number of monitored items per server		3000
Maximum number of subscriptions per server		200
Variable Type		Network Variable
Conditions as a whole network published variables	**Maximum number of variables that can be published**	10000
	Maximum number of value attributes that can be published	10000
Permissible Variables that can be published		Pointer Variables *(M)*, Global Variables *(P)*, EtherCAT IO Data Variables *(Ecat[].Io[].Data)*
OPC UA security mode and policy		Allowable security methods can be specified from the following (multiple specifications possible): • Both signature and encryption required: SignAndEncrypt Signature and encryption algorithm: Basic256-Sha256/Basic256/Basic128Rsa15 (multiple specifications possible) • Only signature required: Sign Signature algorithm: Basic256Sha256/Basic256/Basic128Rsa15 (multiple specifications possible) • Neither signature nor encryption required
Application authentication		X.509
User authentication		The following can be set: • User name and Password • Anonymous

Enabling the OPC UA Server

The OPC UA server on the Power PMAC is enabled by setting saved setup element **UAServer.Enable** to 1. If the saved value of **Enable** is 1, this will happen automatically at power-on/reset.

The settings for the server are established when **UAServer.Enable** is set to 1. If you wish to change any of these settings – for example, the variables to be transferred – **Enable** must be set to 0, and then back to 1.

The setting of **UAServer.Port** when the server application is enabled specifies the Ethernet port number on the Power PMAC that will be used to listen for incoming messages on the OPC UA network.

The setting of **UAServer.EnableUnencr** when the server application is enabled specifies whether unencrypted communications are permitted or not. At its default value of 0, unencrypted communications are not permitted. Unencrypted communications are not recommended in a deployed application, as they result in significant cybersecurity risks.

The setting of **UAServer.EnableAnon** when the server application is enabled specifies whether communications with "anonymous" clients are permitted or not. At its default value of 0, anonymous clients are not permitted. Permitting anonymous clients is not recommended in a deployed application, as this results in significant cybersecurity risks.

The setting of **UAServer.LogLevel** at this time determines what types of messages will be logged.

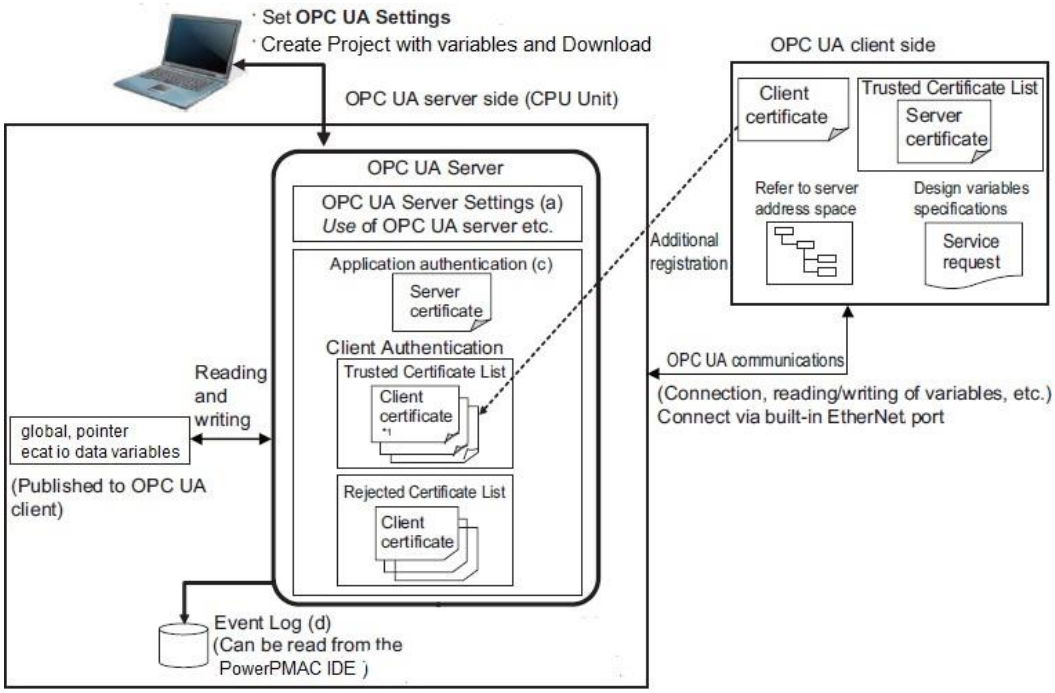
Security Functions of Power PMAC's OPC UA Server

Power PMAC's OPC UA Server supports two key security features of the OPC UA standard. The first is connection authentication, and the second is message security. Use of these security features is not required, but it is strongly recommended.

Connection Authentication

When Power PMAC with connection authentication enabled receives a connection request from an OPC UA client, it only accepts the connection if it has an authentication certificate for this client. Authentication certificates can be installed in the Power PMAC through the IDE.

Similarly, an OPC client can require an authentication certificate from the Power PMAC to accept communications from Power PMAC's OPC UA server.



Connection authentication is required when saved setup element **UAServer.EnableAnon** is set to 0 (the default) when the server operation is started.

OPC UA Login Credential Files

In OPC UA, "Application Authentication" permits applications that want to communicate to identify each other. Each device has a certificate that is exchanged when attempting to establish a "secure channel" of communications. The receiver of the certificate checks it against its own "trust list" to decide whether to accept or reject this request for a secure channel.

A system administrator must determine whether a certificate is properly signed, validated, and trustworthy before placing it the trust list. Associated trust lists contain validated "certificate authorities" and "revoked" certificates that will no longer be accepted.

Power PMAC's required OPC UA login credentials, used if anonymous clients are not permitted, can be found in the **`/opt/ppmac/tools/uaserver/login.txt`** file. Permitted users can be added or removed using the **`uaserver_login`** program located in the **`/opt/ppmac/tools/uaserver`** directory, or via the *OPC UA Login* window of the Power PMAC IDE (which uses this program).

OPC UA TLS Certificates

The TLS (Transport Layer Security) certificate information for Power PMAC's OPC UA Server is found in the **`/opt/ppmac/tools/uaserver/certs`** directory. If this certificate is not already present when the UA Server application is started, it will be automatically generated.

This directory also contains the following folders:

- **`trustlist`**: Contains the certificates of trusted Certificate Authorities and clients.

- **issuelist**: Contains certificates issued by the OPC UA Server itself.

- **revoclist**: Contains the certificates of Certificate Authorities and clients whose access to the OPC UA Server has been revoked.

Message Security

When Power PMAC with message security enabled sends messages to an OPC UA client, it signs the message to identify itself as the source, and encrypts the message to keep it secure from unauthorized devices.

Message security is required when saved setup element **UAServer.EnableUnencr** is set to 0 (the default) when the server operation is started.

OPC UA Data Transfers

Power PMAC's OPC UA Server supports the transfers of 3 types of variables, global (P) variables, pointer (M) variables, and EtherCAT I/O data variables.

Global (P) Variable Transfers

The OPC UA server can enable transfers of up to 20,000 of Power PMAC's global (P) variables. These must be a set of continuously numbered P-variables, starting with the variable specified by the value of **UAServer.PVarBase**, and including the number of these variables specified by **UAServer.PVarNum**.

The default value for **UAServer.PVarBase** of 8192 matches the default starting variable number used in the IDE's project manager for declared global variables. Many users will want to use these defaults, and declare the variables to be available to the server at the top of the project file **global definitions.pmh**.

For example, if the first global-variable declarations in this file are:

```
global CycleCount;
global ReturnTime;
global CutLength;
```

then these variables will be assigned to P8192, P8193, and P8194 by the IDE project manager. If **UAServer.PVarBase** is set to 8192, and **UAServer.PVarNum** is set to 3 or more, these three variables will be made available to the server.

If it is desired to use a combination of declared and defined global variables, the defined variables should be assigned to P-variables just before P8192. To extend the previous example, if we included the following definitions:

```
#define SpindleSpeed    P8191
#define AvgTorque       P8190
```

then if **UAServer.PVarBase** is set to 8190, and **UAServer.PVarNum** is set to 5 or more, these five defined and declared variables will be made available to the server.

Pointer (M) Variable Transfers

The OPC UA server can enable transfers of up to 10,000 of Power PMAC's pointer (M) variables. These must be a set of continuously numbered M-variables, starting with the variable specified by the value of **UAServer.MVarBase**, and including the number of these variables specified by **UAServer.MVarNum**.

The default value for **UAServer.MVarBase** of 8192 matches the default starting variable number used in the IDE's project manager for declared pointer variables. Many users will want to use these defaults, and declare the variables to be available to the server at the top of the project file **`global definitions.pmh`**.

For example, if the first pointer-variable declarations in this file are:

```
ptr ServoCyc->Sys.ServoCount;
ptr Xpos->Motor[1].ActPos;
ptr Ypos->Motor[2].ActPos;
```

then these variables will be assigned to M8192, M8193, and M8194 by the IDE project manager. If **UAServer.MVarBase** is set to 8192, and **UAServer.MVarNum** is set to 3 or more, these three variables will be made available to the server.

If it is desired to use a combination of declared and defined global variables, the defined variables should be assigned to M-variables just before M8192. To extend the previous example, if we included the following definitions:

```
#define XTargetPos      M8190
#define YTargetPos      M8191
XTargetPos->Coord[1].TPData[0].Pos[6];
YTargetPos->Coord[1].TPdata[0].Pos[7];
```

then if **UAServer.MVarsBase** is set to 8190, and **UAServer.MVarsNum** is set to 5 or more, these five defined and declared variables will be made available to the server.

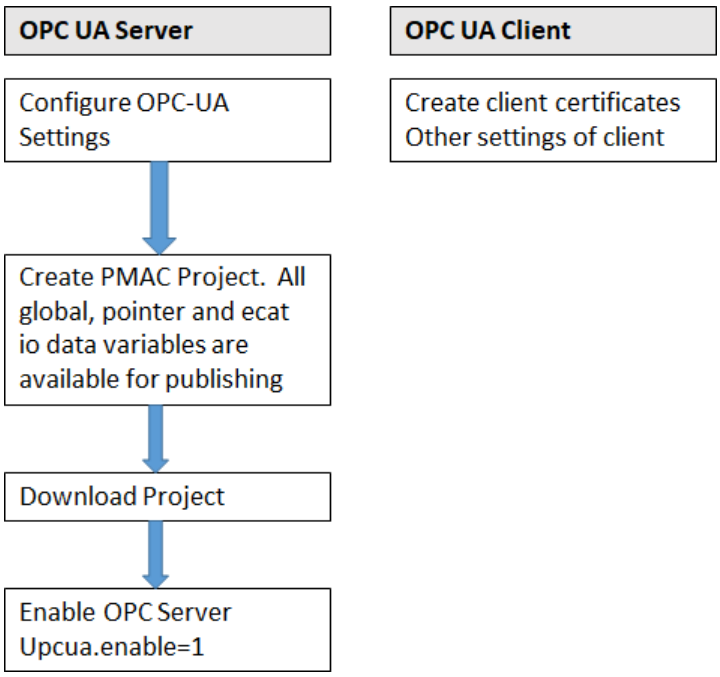
EtherCAT I/O Transfers

The OPC UA server can transfer EtherCAT I/O data registers over the network. If **UAServer.EcatEnable** is set to 1, all active **ECAT[*i*].IO[*k*].Data** registers are made available to the server application. These contain the "process data object" (PDO) values transmitted across the EtherCAT network between Power PMAC and its slave devices each cycle.

This functionality is intended to assist in the monitoring and debugging of the EtherCAT network operation. Generally, it should only be used to let OPC UA clients read this data.

Procedure to Use OPC UA

This diagram shows an overview of the steps needed to use OPC UA on the Power PMAC:



Running the OPC UA Server on Power PMAC

Execute the following steps to enable the OPC UA Server on the Power PMAC:

- Using the Power PMAC IDE (V4.6.4 or newer required), set the Power PMAC parameters for communication with the OPC UA client (first time only). This will set the values of **UAServer** saved setup elements that specify the configuration of the communications, including authentication and encryption.

{Screen capture of IDE Window}

- In the Power PMAC IDE project, use variable declarations or definitions for all pointer (M) and global (P) variables whose values are to be transferred (in either direction) with the OPC UA client. Of course, other variables for the project may be declared or defined as well.

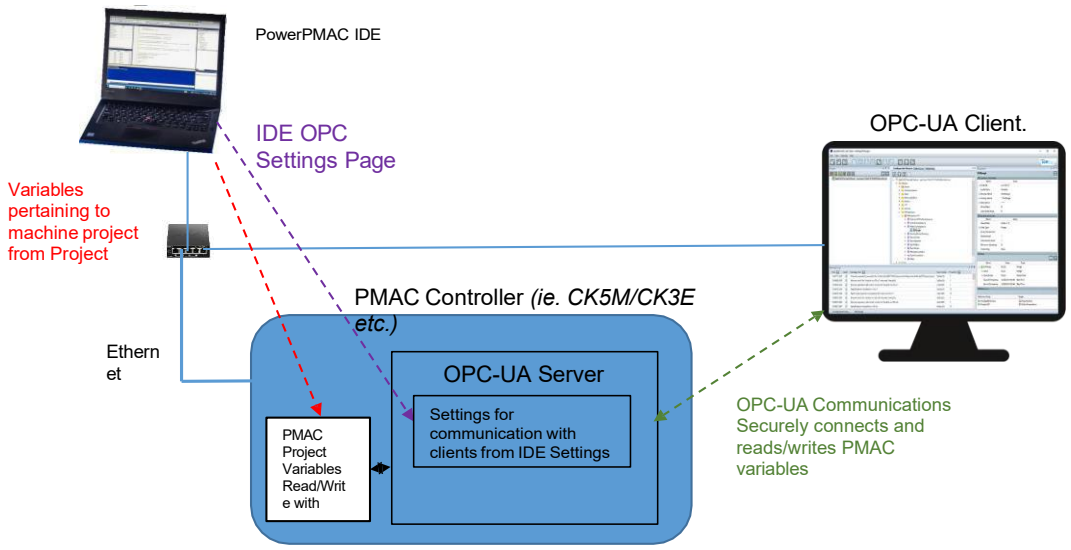
- Download the project to the Power PMAC

- Start the OPC UA server on the Power PMAC by setting **UAServer.Enable** to 1. Communications over the OPC UA network will start.

- Execute a **`save`** command on the Power PMAC if you wish to retain all of this configuration for subsequent sessions.

OPC UA Client

Execute the following steps to enable the OPC UA Client on its device:



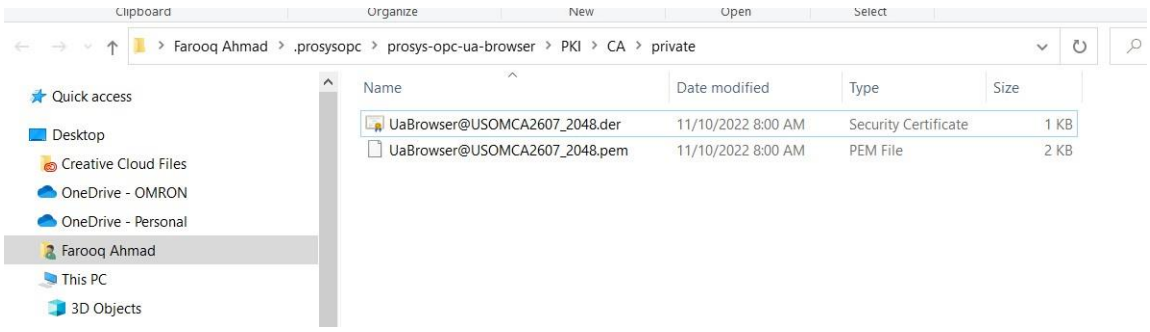
Using an OPC UA Client

This section demonstrates the use of an OPC UA client application to communicate with the Power PMAC server over OPC UA. It uses the B Prosys client application for Windows PCs as an example, but this is not an endorsement of that particular client application.

The client application must be installed on the computer according to the instructions for the application.

If the Power PMAC server requires authentication ("signing"), the client certificate must be copied to the Power PMAC. This only needs to be done once. The instructions to do this are as follows:

First, find the certificate file in a folder associated with the client application. For the Prosys browser, it will look something like this:



Copy this file to the Power PMAC into the folder:

```
/opt/ppmac/tools/uaserver/certs/trustlist/
```

using commands like the following on the Power PMAC and the Windows PC.

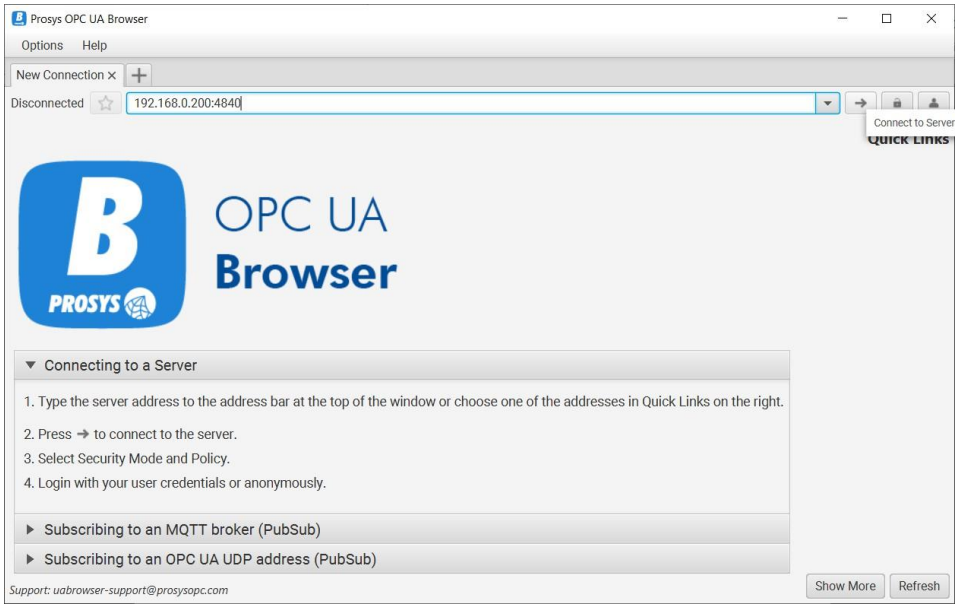
- The first command enables writing to the destination folder on the Power PMAC.
- The second command actually copies the file from the PC's folder to the Power PMAC's folder.
- The third command returns the Power PMAC folder to "read only", protecting it against accidental erasure.

```
On PMAC:
mount -o remount,rw /opt

On windows command:
cd C:\Users\john.doe\.prosysopc\prosys-opc-ua-browser\PKI\CA\private
scp UaBrowser@USOMCA2607_2048.der
      root@192.168.0.200:/opt/ppmac/tools/uaserver/certs/trustlist/

On PMAC:
mount -o remount,ro /opt
```

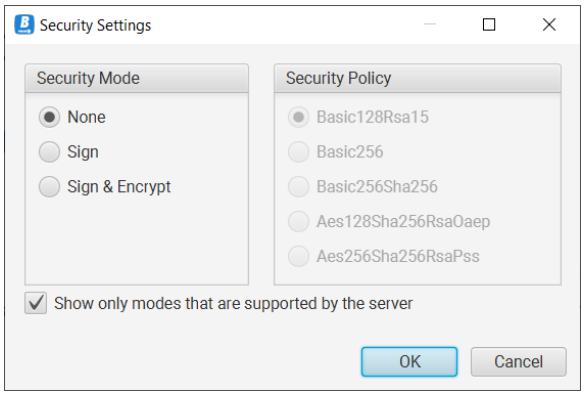
Next, the client application must be launched. An introduction screen like the following will appear:



To link to the Power PMAC, the Power PMAC's IP address must be specified, followed by the port number for the OPC UA communications (default at port 4840), separated by a colon. For the default Power PMAC IP address and port, this would be:

192.168.0.200:4840

Next, a screen like the following appears, asking you to specify the security settings for the communications.



Typically, as in this example, there are three security options:

1. None
2. Sign
3. Sign and Encrypt

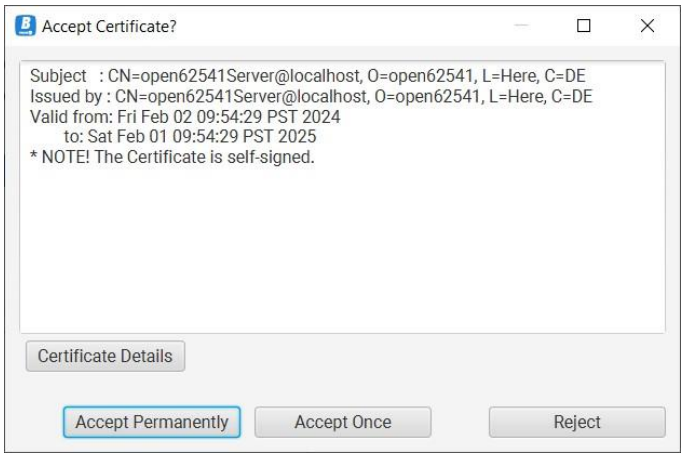
The option you choose must match the option selected for Power PMAC's server.

1. If no security is desired, select "None" and click on "OK".

2. If authentication is desired, but not encryption, select "Sign" and click on "OK".

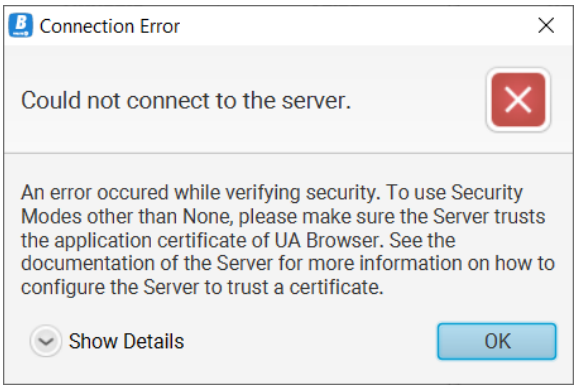
3. If both authentication and encryption are desired, select "Sign & Encrypt", then select the encryption algorithm desired from the right menu, and click on "OK".

If signing has been specified (with or without encryption), a screen like the following will appear, showing the Server's authentication certificate:



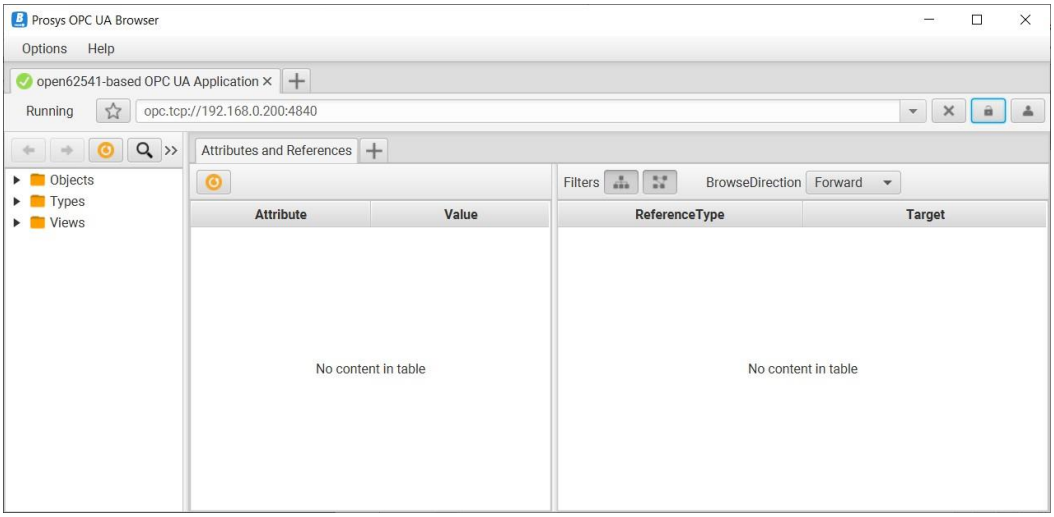
If you select "Accept Permanently", the certificate will automatically be accepted on subsequent launches of the client, and this screen will not appear again.

If the Power PMAC requires an authentication certificate, but does not have a certificate for this client, a screen like the following will appear:

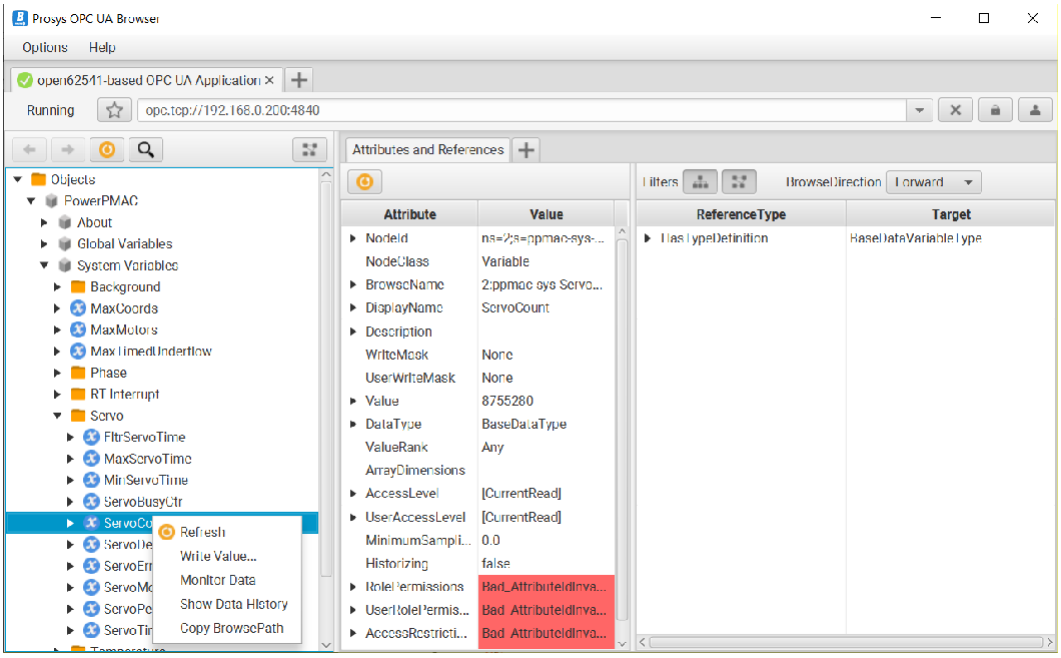


If this is the case, install the client's certificate into the Power PMAC as instructed above.

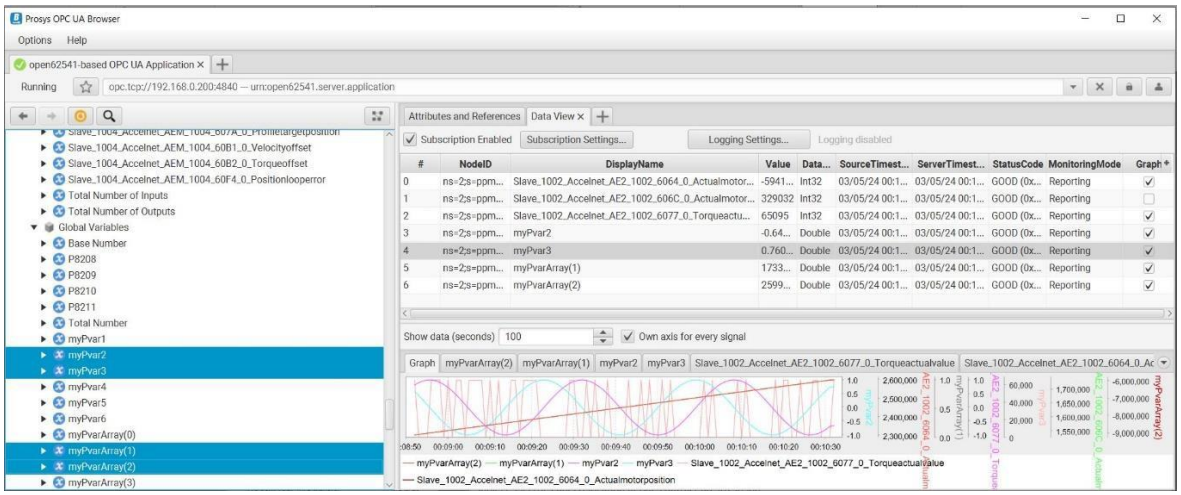
Once communication has been established, with or without authentication or encryption, a screen like the following will appear:



From the left menu, select "Objects", then "Power PMAC", then "Global Variables", "Pointer Variables, or "EtherCAT Variables" to get the category of the desired variable to monitor. Right-click on this variable, and select "Monitor Data" from the pull-down menu.



Now you can monitor the selected variable(s) and plot if desired:



OPC UA Interface Saved Setup Elements

The data structure elements in this section control the operation of the OPC UA Server on the Power PMAC.

UAServer.EcatEnable

Description: OPC UA server EtherCAT I/O transfer enable/disable control

Range: 0 .. 1

Units: Boolean

Default: 0

UAServer.EcatEnable controls whether the mapped EtherCAT I/O data is made available to the OPC UA server application on the Power PMAC or not. If it is set to the default value of 0, the EtherCAT data is not made available.

If it is set to 1, all of the mapped EtherCAT I/O data register values (**ECAT[*i*].IO[*k*].Data**) are made available to the OPC UA server application.

It is the value of **UAServer.EcatEnable** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

UAServer.Enable

Description: OPC UA server enable/disable control

Range: 0... 1

Units: Boolean

Default: 0

UAServer.Enable controls whether the OPC UA server application on the Power PMAC is enabled or not. If it is set to the default value of 0, the application is not enabled.

If it is set to 1, Power PMAC will enable the server application. If the saved value is 1, the application will automatically be enabled on power-up/reset.

The settings for how the server will operate are made by the value of other saved setup elements when the server is enabled, so to change any settings, **Enable** must be set to 0, then set back to 1.

UAServer.EnableAnon

Description: OPC UA server anonymous connection control

Range: 0 .. 1

Units: Boolean

Default: 0

UAServer.EnableAnon controls whether the OPC UA server application on the Power PMAC permits anonymous connections or not. If it is set to the default value of 0, anonymous connections are not permitted, so only authenticated connections can be used.

If it is set to 1, anonymous connections are permitted. This is not recommended for actual operation of the application, as it poses cybersecurity risks.

It is the value of **UAServer.EnableAnon** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

UAServer.EnableUnencr

Description: OPC UA server encrypted/unencrypted message control

Range: 0... 1

Units: Boolean

Default: 0

UAServer.EnableUnencr controls whether the OPC UA server application on the Power PMAC permits unencrypted communications or not. If it is set to the default value of 0, unencrypted communications are not permitted, so only encrypted messages can be used.

If it is set to 1, unencrypted communications are permitted. This setting is not recommended for actual operation of the application, as it poses cybersecurity risks.

It is the value of **UAServer.EnableUnencr** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

UAServer.LogLevel

Description: OPC UA server logging function level control

Range: 0... 5

Units: Enumeration

Default: 2

UAServer.LogLevel controls which messages the OPC UA server application on the Power PMAC logs to /var/log/uaserver#.log (“#” ranges from 0-4) . The following levels can be used:

0: Log trace messages plus messages from higher log levels

1: Log debugging messages plus messages from higher log levels

2: Log info messages plus messages from higher log levels (default)

3: Log warning messages plus messages from higher log levels

4: Log error messages plus messages from higher log levels

5: Log fatal error messages

UAServer.MVarBase

Description: OPC UA server starting M-variable number for transmission

Range: 0 .. 16,383

Units: Variable number

Default: 8192

UAServer.MVarBase specifies the number of the first Power PMAC pointer (M) variable to make available to the OPC UA server application for transmission. **UAServer.MVarNum** specifies the number of consecutively numbered variables starting with this variable to be made available to the application.

It is the value of **UAServer.MVarBase** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

It is generally recommended that the range of M-variables available for use correspond to the M-variables assigned to declared pointer variables in the Power PMAC project. By default, this range starts at M8192.

For example, if **UAServer.MVarBase** is set to 8192, and **UAServer.MVarNum** is set to 200, then M8192 through M8391 would be made available to the application.

UAServer.MVarNum

Description: OPC UA server number of M-variables for transmission

Range: 1 .. 10,000

Units: Variables

Default: 1

UAServer.MVarNum specifies the number of the consecutively numbered Power PMAC pointer (M) variables to make available to the OPC UA server application for transmission. **UAServer.MVarBase** specifies the first of these variables to be made available to the application.

If **UAServer.MVarNum** is set to 0, no M-variables are made available to the server application.

It is the value of **UAServer.MVarNum** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

It is generally recommended that the range of M-variables available for use correspond to the M-variables assigned to declared pointer variables in the Power PMAC project. By default, this range starts at M8192.

For example, if **UAServer.MVarBase** is set to 0, and **UAServer.MVarNum** is set to 80, then M0 through M79 would be made available to the application.

UAServer.Port

Description: OPC UA server Ethernet port number

Range: 0 .. 65,535

Units: Enumeration

Default: 4840

UAServer.Port specifies the number of the Ethernet port the OPC UA server application will use to listen for incoming connections. It is the value of **UAServer.Port** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

UAServer.PVarBase

Description: OPC UA server starting P-variable number for transmission

Range: 0 .. 65,535

Units: Variable number

Default: 8192

UAServer.PVarBase specifies the number of the first Power PMAC global (P) variable to make available to the OPC UA server application for transmission. **UAServer.PVarNum** specifies the number of consecutively numbered variables starting with this variable to be made available to the application.

It is the value of **UAServer.PVarBase** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

It is generally recommended that the range of P-variables available for use correspond to the P-variables assigned to declared global variables in the Power PMAC project. By default, this range starts at P8192.

For example, if **UAServer.PVarBase** is set to 8192, and **UAServer.PVarNum** is set to 100, then P8192 through P8291 would be made available to the application.

UAServer.PVarNum

Description: OPC UA server number of P-variables for transmission

Range: 0 .. 20,000

Units: Variables

Default: 20

UAServer.PVarNum specifies the number of the consecutively numbered Power PMAC global (P) variables to make available to the OPC UA server application for transmission. **UAServer.PVarBase** specifies the first of these variables to be made available to the application.

If **UAServer.PVarNum** is set to 0, no P-variables are made available to the server application.

It is the value of **UAServer.PVarNum** at the time that **UAServer.Enable** is set to 1 that is used as long as the server is enabled.

It is generally recommended that the range of P-variables available for use correspond to the P-variables assigned to declared global variables in the Power PMAC project. By default, this range starts at P8192.

For example, if **UAServer.PVarBase** is set to 8192, and **UAServer.PVarNum** is set to 50, then P8192 through P8241 would be made available to the application.

OMRON Corporation Industrial Automation Company

Kyoto, JAPAN Contact : www.ia.omron.com

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

Cat. No. O086-E-01 0825