Mission Communications LLC

[sales@123mc.com](http://www.123mc.com/demoassisted.asp)

 © 2016 Mission Communications LLC. All Rights Reserved

Mission Communications
OPC UA Server

User Manual

Table of Contents

[2 Introduction 2](#_Toc470012164)

[2.1 Purpose 2](#_Toc470012165)

[2.2 Overview 2](#_Toc470012166)

[3 Mission OPC UA Server 3](#_Toc470012167)

[3.1 Using Mission OPC UA Server 3](#_Toc470012168)

[3.1.1 Requirements for a Data Linkage 3](#_Toc470012169)

[3.1.2 Connecting to Mission OPC UA Server 3](#_Toc470012170)

[3.1.3 OPC UA Client 4](#_Toc470012171)

[3.1.4 UA Proxy 4](#_Toc470012172)

[3.1.5 Server Endpoints 4](#_Toc470012173)

[3.1.6 Local Discovery Server 5](#_Toc470012174)

[3.1.7 Testing or Troubleshooting OPC UA Connection 5](#_Toc470012175)

[3.2 Security 5](#_Toc470012176)

[3.2.1 Security Policy 6](#_Toc470012177)

[3.2.2 Message Security Modes 6](#_Toc470012178)

[3.2.3 User Token Type 7](#_Toc470012179)

[3.2.4 X.509 Certificate 7](#_Toc470012180)

[3.2.5 VPN Security 9](#_Toc470012181)

[3.3 Server Object 9](#_Toc470012182)

[3.4 RTU Additions After a Connection Is Established 10](#_Toc470012183)

[4 OPC Nodes 10](#_Toc470012184)

[4.1 Attributes and Metadata 10](#_Toc470012185)

[4.2 OPC Node Definitions 12](#_Toc470012186)

[5 Remote Control of RTUs 13](#_Toc470012187)

[6 Comparison with Mission OPC Driver 13](#_Toc470012188)

[6.1 OPC UA for Current Mission OPC Users 15](#_Toc470012189)

[7 Frequently Asked Questions 15](#_Toc470012190)

[8 Glossary 17](#_Toc470012191)

[9 Mission OPC UA Server Status Codes 18](#_Toc470012192)

# Introduction

## Purpose

This document provides an overview of Mission Communications OPC UA Server and instructions on establishing data linking between Mission data servers and a local SCADA-HMI system. Furthermore, this document provides detailed steps for troubleshooting of errors and problems that might be encountered while using OPC UA Server.

This document covers:

Mission OPC UA Server:

* Version 1.0 (November 2016) BETA

Mission OPC UA Server is a replacement connection method for the Mission OPC Driver (versions 6.0 and 5.0) that connected to the Mission Enterprise Server and includes all data nodes presented through the Driver plus a few new data nodes and methods. Node names and addresses in Mission OPC UA Server are slightly different from the Mission OPC Driver.

## Overview

The primary challenge of data linkage is getting data through firewalls and into the SCADA-HMI software while protecting the enterprise from unauthorized users.

The Mission M800, M110 and Manhole Monitor Remote Terminal Units (RTU) send data into Mission Communications secure computer center on a periodic basis (2 minute, 1 hour, and 1-3 day periods, respectively). The data is processed and stored indefinitely and can be accessed by SCADA-HMI software through the Mission OPC UA Server.

Mission OPC UA Server fully complies with version 1.03 (10 October 2015) of OPC UA standard as defined by the OPC Foundation. OPC Unified Architecture (UA) is an industrial communication protocol developed by the OPC Foundation as a successor to the OPC Classic protocol. It features all functionality from and backwards compatibility to OPC Classic while providing new features like multi-platform support and increased security. Many commercial SCADA-HMI packages like WonderWare have an integrated OPC UA client while packages with OPC Classic clients, can utilize UA Proxy middleware to connect to Mission OPC UA Server. More information on OPC UA including specifications is available from the OPC foundation (https://opcfoundation.org/).

Data from Mission RTUs is stored on Mission data servers; therefore, the Mission Managed SCADA system continues to be available for viewing data, configuring settings, and all other functions. Some OPC users use Mission solely for telemetry and utilize their SCADA-HMI for alarming and reporting. Others take a hybrid approach that can take many forms. For example, some utilities utilize Mission’s event alarming functionality and their traditional system as a historian. Others use Mission as a “warm” backup system and only enable Mission alarm callout functions when needed.

Most data that is available from the OPC link is the actual RTU data, not the interpreted data (reports) available from the Mission web portal. The listings of the specific nodes that are transmitted are in the attached spreadsheet OPCNodeVx.xls.

Customers who have Mission units associated with two or more “accounts,” can use one OPC UA client to retrieve data from both accounts. For instance, data on websites such as YourCityWater and YourCityWasteWater can be managed with one client. This feature offers the convenience of collecting and managing information all in one place. Customers with redundant SCADA-HMI systems can also be accommodated by this method.

# Mission OPC UA Server

Mission OPC UA Server is an OPC UA server that is secured by and resides behind Mission firewalls. The server allows access to data from Mission servers using **opc.tcp** protocol as described in the OPC UA specifications. It supports multiple security features including authentication, encryption, signing, and user access control.

## Using Mission OPC UA Server

### Requirements for a Data Linkage

1. A Mission Customer account with at least one RTU.
2. A SCADA-HMI that supports OPC UA or OPC Classic with UA Proxy middleware.
3. Outbound Internet access from a Customer’s local server that will be running SCADA-HMI or UA Proxy. The router associated with the network that hosts SCADA-HMI or UA Proxy must allow **opc.tcp** protocol to port **4840**.
4. Mission OPC Login credentials (available from Mission Tech Support). For testing purposes, Technical Support can provide you with both a production and test credential set. There is no functional difference between the test credentials and the production ones.

### Connecting to Mission OPC UA Server

The connection between your SCADA-HMI and the Mission OPC UA Server is performed from within your SCADA-HMI; therefore, only general guidelines can be provided.

1. Configure your SCADA-HMI or UA Proxy middleware to utilize the OPC UA protocol and connect to Mission OPC UA Server using the URL and port provided.
2. Select the desired level of security and encryption. Please note that not all security features supported by Mission OPC UA Server are supported by all OPC UA clients.
3. Enter the provided Mission OPC username and password. Local X.509 certificate is required for this even if no security is selected for communication.
4. Upon a successful connection, the OPC UA client might prompt for the acceptance of Mission OPC UA Server’s X.509 certificate. The certificate must be accepted for successful communication.
5. Define the specific nodes (RTU data points) that are of interest. Some SCADA-HMIs require to first create notification containers called groups. Then the specific OPC nodes are assigned to the group(s).
6. The Integrator or SCADA-HMI specialist can present the data graphically and perform alarming functions as desired.

### OPC UA Client

An OPC UA Client that is a component or plug-in of the SCADA-HMI is the recommended solution to connecting with Mission Communications OPC UA Server. With a native client, only the OPC UA connection needs to be configured and most UA clients provide advance UA features live multiple timestamps and method calls (commands).

### UA Proxy

For existing Mission Communications OPC clients and HMIs without native OPC UA support, third-party middleware called **UA Proxy** can be employed to translate data between OPC UA server and OPC Classic client. This software is available from multiple manufactures with a range of features and prices.

The following UA Proxy solutions have been tested and verified as working with Mission Communications OPC UA Server:

* **Kepware KEPServerEX 5/6 Communications Suite** offers an OPC UA client package that allows secure communication with OPC UA Server including live data changes.
* **Matrikon MatrikonOPC UA Proxy** allows secure communication with OPC UA Server including live data changes.
* **Unified Automation UaGateway** allows secure communication with OPC UA Server including live data changes and timestamp updates without data. It also supports Windows XP SP3 and Windows Vista.

### Server Endpoints

Mission OPC UA Server provides the following endpoints where clients can connect to:

|  |  |  |  |
| --- | --- | --- | --- |
| Endpoint URL | Security Policy | Message Security Mode | User Token Type |
| opc.tcp://opcus.123mc.com:4840/ | Basic256Sha256 | SignAndEncrypt | Username |
| opc.tcp://opcus.123mc.com:4840/ | Basic256Sha256 | Sign | Username |
| opc.tcp://opcus.123mc.com:4840/ | Basic256 | SignAndEncrypt | Username |
| opc.tcp://opcus.123mc.com:4840/ | Basic256 | Sign | Username |
| opc.tcp://opcus.123mc.com:4840/ | Basic128Rsa15 | SignAndEncrypt | Username |
| opc.tcp://opcus.123mc.com:4840/ | Basic128Rsa15 | Sign | Username |
| opc.tcp://opcus.123mc.com:4840/ | None | None | Username |

In addition, Mission Communications provides a Discovery Server, located at the same URL as the OPC UA Server, which can be utilized to retrieve a list of available endpoints with their security configuration.

In order for a client to connect to an endpoint, the same security configuration must be supported.

### Local Discovery Server

Mission Communications provides access to a Local Discovery Server (LDS) that publically exposes all available endpoints of the Mission OPC UA Server to the client. An OPC UA Client that supports LDS can browse the URL of the Mission OPC UA Server to see the endpoints and their configured security.

### Testing or Troubleshooting OPC UA Connection

#### OPC UA Client

A stand-alone OPC UA client is recommended for testing or troubleshooting the connection to Mission OPC UA Server. The most advance free OPC UA client is UaExpert from Unified Automation GmbH available for Windows, multiple distributions of Linux, and Android mobile OS. It supports the latest OPC UA specification 1.03 and allows for security testing, reading and writing of data nodes, and calls to OPC methods. Other free OPC UA clients are available from Integration Objects, CommServer, Inductive Automation, and Prosys. The OPC Foundation also provides multiple OPC UA clients for members with a valid login.

#### Ping

If OPC UA connection is not established with a stand-alone OPC UA client, it is possible to ping Mission OPC UA Server. This can be done from a Command Prompt in Windows, Network Utility or Terminal in Mac OS, or Terminal in Linux/UNIX. The ping should be sent to the server’s endpoint URL without the **opc.tcp** prefix or the port number. For example, if the endpoint URL is **opc.tcp://opcus.123mc.com:4840/**, the ping command in the Command Prompt or Terminal would be **ping opcus.123mc.com**. If the ping receives a reply, OPC UA component of server could be down or OPC UA communications could be blocked by a firewall or router; otherwise, the entire server or its network component could be offline or communication to the server disabled. In either case, Mission Communications Technical Support should be contacted.

**Note:** Endpoint URL could be different if VPN is used. For VPN clients, connection attempt should be made outside the private network to the public endpoint URL in order to bypass potential VPN issues.

**Note:** The **ping** command is disabled or blocked on some networks. A ping to [www.google.com](http://www.google.com) or [www.yahoo.com](http://www.yahoo.com) should receive a reply if the **ping** command is enabled and the network is functioning properly.

## Security

Mission OPC UA Server offers extensive built-in security known as UA Secure Conversation. This includes:

* **Authentication** with X.509 certificates for both client and server before connection is allowed.
* **Session Encryption** where all messages are encrypted with 128 or 256 bit encryption before transmission.
* **Message Signing** where all messages are signed to ensure that they are received exactly as they are sent.
* **Sequenced Packets** reduce opportunities for message reply attacks.
* **User Access Control** requires user authentication before a connection can be established and further restricts access to individual data.
* **Auditing and Logging** of all user activities.

Mission OPC UA Server is designed to make firewall configurations much easier especially on the client side. It uses port 4840, the official OPC UA port, for incoming client communication; therefore, the client should have this port open for outgoing **opc.tcp** protocol messages. Likewise, any client-specific port(s) should also be allowed. Please see the client’s user’s manual for required firewall configuration.

### Security Policy

Mission OPC UA Server supports the following security policies used for message encryption as defined by the OPC Foundation:

|  |  |
| --- | --- |
| Security Policy | URI |
| Basic256Sha256 | <http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256> |
| Basic256 | <http://opcfoundation.org/UA/SecurityPolicy#Basic256> |
| Basic128Rsa15 | <http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15> (not recommended) |
| None | <http://opcfoundation.org/UA/SecurityPolicy#None> (not recommended) |

**Note:** Mission Communications recommends that **Basic256Sha256** or **Basic256** encryptions be used for highest level of message security.

### Message Security Modes

Mission OPC UA Server supports the following message security modes for each message between the client and the server:

|  |  |
| --- | --- |
| Security Mode | Description |
| SignAndEncrypt | All messages are signed and encrypted |
| Sign | All messages are signed but not encrypted |
| None | No message security (not recommended) |

Message signing means that all messages are signed to ensure that they are not modified or corrupted during transport.

Message encryption means that are encrypted using public and private keys to ensure that they are not read by a third-party if intercepted during transport.

### User Token Type

Mission OPC UA Server supports the following user identity tokens for user verification:

|  |  |
| --- | --- |
| User Token Type | Description |
| Username Identity Token | User is identified by a username and password.(RTU data is available) |
| Anonymous Identity Token | No user information is provided.(No RTU data is available) |

**Note:** Username and password are issued by Mission Communications and may differ from those used to access 123Scada or 123mc. They are the only way to access RTU data. Anonymous access to the OPC UA Server is allowed only for diagnostic purposes. It can be used to verify firewall settings and server connection status but cannot be used to access Mission Data Center to receive RTU data.

**Note:** Certificate token type and other token types are not supported.

### X.509 Certificate

OPC UA security requires both client and server to exchange and validate X.509 Version 3 application instance certificates. Each X.509 certificate consists of a public key exchanged between the server and client, a private key that is known only to the local application, and the information stored in the certificate that identifies the owner and specifies how long the certificate is valid and what level of security the owner supports.

On first connection, the client and the server exchange their public keys and each application must trust the public key of the other. On the client side, a dialog similar to the one in the image might appear to trust the server’s public key.



Check Server Certificate

(Source: http://documentation.unified-automation.com/uaexpert/1.4.2/html/first\_steps.htm)

If the key is not trusted, secure connection is not possible. In certain circumstances, the server’s untrusted public key might automatically be placed in the client’s untrusted directory or certificate store. This might require the public key to be manually moved or copied to the trusted directory and deleted from the untrusted directory. Once both sides trust the exchanged public keys, the client and server establish a secure channel where all messages, including username and password, are signed using the private key and encrypted using the public key.

Without a valid X.509 certificate, only anonymous connection with no security is possible. This can be used for network troubleshooting and to determine the server’s connection status, but cannot be used to access any customer or RTU data.

**Note:** All commercial OPC UA products (clients and proxies) should include an X.509 certificate or a way to generate one. Mission Communications cannot provide or assist in acquiring a 3rd party X.509 certificate.

### VPN Security

Mission Communications offers a Virtual Private Network (VPN) option with 128-bit AES encryption for additional security. The VPN feature requires a compatible VPN endpoint at the customer’s premises to establish a secure connection with the Mission’s endpoint. When using VPN, OPC UA Server’s endpoints may differ and new endpoints will be provided by Mission Technical Support. All encryption and security options will still be available as they are independent of VPN connection.

**Note:** VPN is not required to access Mission OPC UA Server.

## Server Object

Mission OPC UA Server provides a server object that defines the capabilities supported by the OPC UA Server and exposes the server’s current state. The intended usage is defined in Part 4 of the OPC UA Specification and is recommended for diagnostic and troubleshooting purposes.



Server Object in UaExpert OPC UA Client

|  |  |
| --- | --- |
| Server Attribute | Description |
| Variable ServerStatus | Contains elements that describe the status of the Server including State, CurrentTime, StartTime, and Buildinfo.**Note:** State = 0 means that the server is running normally. |
| Variable ServiceLevel | Describes the ability of the Server to provide its data to the client from 0 (worse) to 255 (best). |
| Object ServerCapabilities | Defines the capabilities supported by the OPC UA Server. |
| Object ServerDiagnostics | Defines diagnostic information about the OPC UA Server.  |
| Object VendorServerInfo | Displays the license and owner of the OPC UA Server. |
| Method RequestServerStateChange | Allows a Client to request a state change in the Server.**Note:**  Administrator access required. |

**Note:** Server methods require administrator access.

## RTU Additions After a Connection Is Established

Mission OPC UA Server provides an OPC method called “Refresh” in each Customer folder along with RTU objects. This method is called by an OPC UA Client without parameters and reloads all RTUs and RTU data from Mission Data Center. If OPC UA client in SCADA-HMI or UA Proxy does not support methods calls, a free third-party OPC UA Client, UaExpert, can be used to call the method once a connection is established. Finally, Mission Tech Support can call the “Refresh” method remotely. Reconnection to Mission OPC UA Server is not necessary.

# **OPC Nodes**

OPC UA architecture is based on nodes, also called tags in OPC Classic, that are objects with attributes like read/write access level and metadata like timestamps.

## **Attributes and Metadata**

The following is an example of node attributes and metadata for an analog input value from UaExpert OPC UA client.

**Node:** Not all OPC UA clients or UA Proxy middleware support all node attributes.



OPC UA Node Attributes in UaExpert OPC UA Client

|  |  |
| --- | --- |
| Node Attribute | Description |
| NodeId | Specifies a unique ID of the node including its location in the RTU as related to other nodes. The Identifier of the NodeId includes the customer’s name and the serial number of the RTU. |
| DisplayName | The name of the node as it is displayed to the OPC UA client. For example “ScaledValue” or “Value”. |
| Description | Textual description of the node and its value. |
| DataType | The data type of the node such as integer, float, Boolean or string. |
| SourceTimestamp | The timestamp of the last value update in the Mission Data Center. This could correspond to the last time the value changed or the last time the RTU communicated with Mission.**Note:** When monitoring or subscribing to a node, OPC UA clients and UA Proxy middleware should be set to use this attribute in addition to value and status as a data change trigger. |
| ServerTimestamp | The timestamp of the last value update in the OPC UA Server. This could correspond to source timestamp for new updates or the first time the OPC client accessed the server and got the data from the Mission Data Center. This value could be manually updated with a forced read. |
| StatusCode | Indicates the status of the node. “Good” indicates that the status in both current and valid. “Bad” indicates a problem with the server, node, or value. |
| AccessLevel | Specifies if the node can be read or written. “CurrentRead” means that the OPC client can read the value. “CurrentWrite” indicates that the OPC client can write a new value to the node.  |
| UserAccessLevel | Indicates AccessLevel for the current user. |
| MinimumSamplingInterval | Specifies how fast the OPC UA server can detect value changes (usually in milliseconds). Polling of this node should not be done faster than this.**Note:** Mission recommends that polling be set between 5 and 10 seconds. **Node:** MinimumSamplingInterval indicates the minimum allowed polling for this node. The actual update may be done faster and does not take account of the Mission data center. |
| Executable | **Method nodes only.** Indicates if the method can be invoked at this moment. |
| UserExecutable | **Method nodes only.** Indicates if the current user can invoke this method. |

## **OPC Node Definitions**

Please see OPC UA NodesVX.xls spreadsheet for a full list of nodes and other notes.

# Remote Control of RTUs

In addition to accessing RTU data, Mission OPC UA Server allows remote control of RTUs from local SCADA-HMI through writable nodes. Commands to change state can be written into output replay set point nodes and raw analog output values can be written into analog output set point nodes. Actual current values of each output is also available in corresponding value nodes for each output. When a new value is written into a node, it is sent by the OPC UA Server to the Mission data center to be paged to the RTU.

**Note:** OPC UA Server does not modify RTU state directly. All commands are paged to the RTU from the Mission Data center.

Most importantly, when using remote control, fail-safe systems must be designed for failure modes when any or all of the devices involved in the control logic go off line, come on line, or lose power for any reason. Remote control should never replace or supersede local control. Furthermore, remote RTU control with OPC UA bypasses business rules and logic included in Mission’s automated remote control systems like “Tank and Well” and “Positive-Relay-Feedback”. Please see Mission document “Best Practices for Remote Control Applications” business logic considerations when remotely controlling RTUs.

It is vital that integrators design fail-safe systems when commands are initiated. This includes failure modes when any or all of the devices involved in the control logic go off line, come on line, or lose power for whatever reason. Because of the nature of remote communications, remote control should never replace or supersede local control.

**Note**: The Mission system should not be used as a virtual PLC for control applications that require relatively frequent cycles or relatively tight timing precision such as lift station control. Mission Communications reserves the right to add service fees for excessive data usage.

# Comparison with Mission OPC Driver

Mission OPC UA Server leverages the latest technology to offer multiple benefits over Mission OPC Driver and Mission Enterprise Server.

|  |  |  |
| --- | --- | --- |
|  | Mission OPC UA Server | Mission OPC Driver/Enterprise Server |
| Protocol | OPC UA 1.03 (10 Oct. 2015) | OPC DA 2.0 (13 Oct. 1998) |
| Security | X.509 AuthenticationSession encryptionMessage signingUsername / PasswordVPN | Username / PasswordVPN |
| Platform / OS | Any (Windows, OS X, Linux/UNIX, Android …) | Windows Only |
| Local Installation | None (middleware may be required for DA clients) | Mission Driver |
| RTU Refresh | OPC method | Mission Technical Support |
| Alarm Acknowledge | OPC method | N/A |
| Troubleshooting | 3rd-party OPC UA ClientsPingMission Technical Support | Mission Technical Support |



Mission OPC UA Network Architecture



Mission OPC Classic Network Architecture

## OPC UA for Current Mission OPC Users

Two upgrade paths are available for current Mission OPC users desiring to switch to OPC UA.

First, many SCADA-HMIs support OPC UA clients that can connect directly to Mission OPC UA Server. This is the preferred solution as it does not require the installation of 3rd-party middleware and may provide better support of OPC UA features like methods and source timestamps. Due to changes in OPC node addressing, remapping of OPC nodes to variables will be required.

Second, for SCADA-HMIs that do not support native OPC UA clients or for customer who do not desire to use a separate OPC UA client, a middleware called UA Proxy may be utilized to retrieve data from Mission OPC UA Server and convert it into OPC DA format for consumption by OPC DA clients. UA Proxy software is available from many companies with assorted features and options. Some proxy software also supports mapping of OPC UA variables to OPC DA allowing SCADA-HMI software to work with current node configurations.

# Frequently Asked Questions

**How does the SCADA-HMI know if the M110 RTU has an analog in alarm?**

M110 RTUs send in analog values hourly, or when an analog threshold (stored on the RTU) is breached. Therefore the Mission web portal should be used to set the analog alarm threshold values for M110 RTUs. This action insures that the RTU receives the analog alarm set points so that analog data is transmitted immediately when the value goes out of bounds. Please see the question on Analog inputs 3-6.

**Are there any differences when using the Analog Input Option Board?**

Alarm set points are not stored on the RTU for the inputs on the analog expansion board (AN3-6); however, M800 RTUs report analog values every 2 minutes (or when value changes more than 5%) therefore an out of bounds analog value will be available in the Mission system or your HMI in a timely fashion. M110s send in analog values hourly. The M110 should not be used in applications requiring alarming on the expanded analog inputs other than slowly changing values like the level of a large reservoir.

**How do I know if an input is in alarm?**

This requires knowing if the input is configured as NO or NC at the Mission web portal as well as looking at the actual state of the input. With the default configuration of inputs (NO), a closed contact is an alarm indication. A closed contact shows as a 1.

**Can an alarm be dispatched (called out) from the Mission system but acknowledged using the HMI?**

Yes, the alarm notification can be dispatched and acknowledged using the Mission system and acknowledged using Mission OPC UA Server through a method call. The alarm will show as unacknowledged on the Mission system and the entire call out schedule will be executed in this case.

**We want to utilize the Mission system for alarm call outs and acknowledgements, but want some way for our Operations Center to be notified if there are any orphaned alarm events. Are there provisions for such a workflow?**

Yes, a node is available that shows the number of alarm events that have not been acknowledged on the Mission system for each RTU for the past seven days. Generally, it will be zero, so business logic in your HMI can utilize this node to highlight non-zero situations. From a practical standpoint, staff members should be allowed reasonable time to acknowledge the alarm before your control room staff elevates the situation.

**Do I have to use Mission’s alarm notification system?**

No. If you choose to use your HMI for alarm notifications, it is suggested that RTUs be disabled for alarm call outs at the Mission web portal.

**How often does the OPC server update its data?**

For most data, Mission OPC UA publishes it to clients as soon as it becomes available. However, some data like descriptions are polled by the server from Mission Data center every two minutes. Within the OPC UA Client, sampling interval of 5-10 seconds is recommended.

**How to determine when data was last updated?**

In addition to value, each OPC UA node provides two timestamps. The server timestamp indicates when the server last published the value while the source timestamp indicates when the value was last created in the Mission Data Center. For example, if an input value last updated yesterday but the OPC UA client connected to the server today, the server timestamp will show the time of the server connection (today) whereas the source timestamp will show the time of the last update (yesterday). For some live data, source time stamp will update every time the RTU sends data even if the data itself did not change.

# Glossary

**COM** – Component Object Model is a proprietary Microsoft technology for communication between software components utilized by OPC Classic.

**DCOM** – Distributed Component Object Model is a proprietary Microsoft extension of COM for communication between COM components over a network.

**HMI** – Human Machine Interface is a user interface that allows control and feedback between electrical or mechanical devices and a human operator.

**LDS** – Local Discovery Server is a software that publically exposes all OPC servers and their endpoints on a given computer. For OPC UA, LDS is located on port 4840.

**OPC** – Open Platform Communications is a series of standards and specifications for industrial telecommunications and automation.

**OPC Foundation** – industry consortium that creates and maintains standards and specifications for open connectivity between industrial devices and systems.

**OPC Classic** – OLE for Process Control is a series of standards and specifications for industrial communications created by the OPC Foundation and based on the OLE, COM, and DCOM technologies developed by Microsoft for Microsoft Windows operating system.  It is currently being superseded by OPC UA.

**OPC DA** – OPC Data Access is a subset of OPC Classic that deals with reading and writing of real-time data.

**OPC HDA** – OPC Historical Data Access is a subset of OPC Classic that deals with reading of archived data.

**OPC AE** – OPC Alarms and Events is a subset of OPC Classic that deals with exchange of alarm and event messages as well as state management.

**OPC UA** – OPC Unified Architecture is a series of standards and specifications for industrial communications created by the OPC Foundation to eliminate the need to use DCOM technology in order to allow implementation in non-Windows environments, easier connectivity, and combine functionality of existing OPC interfaces.

**RTU** – Remote Terminal Unit is a microprocessor-controlled device that interfaces objects in the physical world to a distributed control or SCADA system.

**SCADA** – Supervisory Control and Data Acquisition is a system that provides control of remote devices from a central location typically using an HMI.

**UA Proxy** – Software that works as a middleware and contains an OPC UA client and an OPC Classic server to convert data from an OPC UA server for consumption by OPC Classic clients. It is the opposite of UA Wrapper.

**UA Wrapper** – Software that works as a middleware and contains an OPC Classic client and an OPC UA server to convert data from an OPC Classic server for consumption by OPC UA clients. It is the opposite of UA Proxy.

# Mission OPC UA Server Status Codes

|  |  |  |
| --- | --- | --- |
| Status Code | Description | Troubleshooting |
| Good | Operation successful |  |
| BadUserAccessDenied | Access denied for current login | 1. Check that username and password are correct.
2. Contact Mission Tech Support.
 |
| BadIdentityTokenRejected | Attempting to connect without using username and password (ex. User Token set to Certificate or Active Directory) | 1. Check that OPC UA Client is set to use Username User Token type.
2. Check that username and password are correct.
3. Contact Mission Tech Support.
 |
| BadIdentityTokenInvalid | Invalid username or password (ex. Username or password are blank of white space) | 1. Check that username and password are correct.
2. Contact Mission Tech Support.
 |
| BadNotImplemented | Requested operation is not implemented | 1. Contact Mission Tech Support.
 |
| BadNotReadable  | User access level does not allow reading of the node or the node is not readable | 1. Check that the node is readable.
2. Check that username and password are correct.
3. Contact Mission Tech Support.
 |
| BadNotWritable  | User access level does not allow writing of the node or the node is read-only | 1. Check that the node is writable.
2. Check that username and password are correct.
3. Contact Mission Tech Support.
 |
| BadOutOfRange  | The value of the node is out of allowed range (too big or too small) | 1. Check if the value correspond to the node type.
2. Contact Mission Tech Support.
 |
| BadMethodInvalid | Error calling a method | 1. Contact Mission Tech Support.
 |
| BadNodeIdUnknown | Trying to access a node that does not exist | 1. Wait a few minutes before trying to access again.
2. Call Refresh method and wait until all RTUs are loaded before trying to access the node.
3. Contac Mission Tech Support.
 |
| BadCommunicationError | Unable to connect to the server | 1. Check if connection works with UaExpert or another OPC UA Client.
2. Check if network connection exists from SCADA-HMI to OPC UA Server.
3. Check if network connection exists to OPC UA Server from another location outside of the firewall.
4. Contact Mission Tech Support.
 |
| BadCertificateUntrusted  | The X.509 Certificate provided by the OPC UA Server was not trusted by the client | 1. Check if the SCADA-HMI package has an option to trust the OPC UA Server’s certificate.
2. Check if the X.509 certificate from the OPC UA Server is in the Trusted or Rejected directory or certificate store.
3. If the certificate is in the Rejected directory, move it into the Trusted directory.
4. Contact Mission Tech Support.
 |
| BadCertificateTimeInvalid | The X.509 Certificate provided by the OPC UA Server has expired | 1. Contact Mission Tech Support.
 |
| BadCertificateIssuerTimeInvalid | The X.509 Certificate provided by the OPC UA Client has expired | 1. Create or purchase new certificate.
2. Contact OPC UA Client or OPC UA Proxy support for new certificate.
 |
| BadCertificateIssuerRevoked | The X.509 Certificate provided by the OPC UA Client has been revoked | 1. Create or purchase new certificate.
2. Contact OPC UA Client or OPC UA Proxy support for new certificate.
 |