SARTORIUS

Connecting Biobrain® Supervise to Ambr® Bioreactors via OPC Unified Architecture (UA)

Martin Wehrhahn, Hareesh Konanki
Sartorius Stedim Systems GmbH, Robert-Bosch-Straße 5-7, 34302 Guxhagen

Contact: biobrain.supervise@sartorius.com

Abstract

Biobrain® Supervise, from version 4.9 onward, offers a straightforward method to connect to Ambr®-powered devices via its built-in OPC Unified Architecture (UA) client, enabling secure connections with instruments or systems that provide OPC UA servers.

This application note provides guidance on establishing a secure connection between Biobrain® Supervise and Ambr® 15 using OPC UA for supervisory control and data acquisition.

Introduction

OPC Unified Architecture (UA) is an open standard communication protocol for industrial automation developed by the OPC Foundation. It is manufacturer-independent and can be used for different kinds of data exchange (i.e., machine to machine, machine to PC, PC to PC). Biobrain® Supervise is a supervisory control and data acquisition (SCADA) system, and in version 4.9, an OPC Unified Architecture (UA) client was introduced into the software, allowing easy connection to bioreactor OPC UA servers.

The Ambr® 15 system is an automated, high-throughput bioreactor system equipped with 24 or 48 fully single-use 15 mL bioreactors, available with or without cooling. It is used across a range of applications, including process development, process optimization, scale-down studies, and both cell culture and microbial fermentation. Ambr® bioreactors are powered by the Ambr® automation platform, engineered to support rapid adaptation of a biomanufacturing facility to address evolving process needs. The Ambr® platform provides an optional OPC UA server (Kepware® OPC UA Server) to enable connections to other SCADA, distributed control system (DCS), or historian systems.

This application note provides guidance for configuring a secure OPC UA connection between Biobrain® Supervise and bioreactors powered by the Ambr® automation platform, using Ambr® 15 as an example.

Methods

Prerequisites

Biobrain® Supervise must be running version 4.9 or newer with a licensed OPC UA client module, and the bioreactor must be connected to the same network. In the context of this application note, the bioreactor must be configured for local user management and use a static IP address. Both systems are assumed to operate with their default self-signed OPC UA application certificates. Traffic via TCP port 4840, as used by the OPC UA server, must be permitted by the respective firewalls.

Bioreactor configuration for Ambr® 15

Step 1: Verifying the time zone is correct

Log in to the Ambr® 15 computer system using an account with administrative privileges. Open the computer's Date and Time section. Verify that the currently selected time zone of the Ambr® 15 computer and Biobrain® Supervise computer match.

Step 2: Preparation of the Ambr® 15 bioreactor configuration

Once the Ambr® 15-related software is installed according to the installation guide, it should be licensed with a new footprint provided by the Ambr® team. Confirm the license is valid before proceeding.

The OPC interface is a separately licensed, optional feature of the Ambr® 15 software. To obtain a new license, please contact TAP support at Sartorius. The license file supersedes any pre-existing license file and should be placed in the C:\AMBR\BIn folder.

The Ambr® 15 runtime application and Kepware® OPC server use global shared memory to exchange data. To facilitate this, a shared memory service must be installed by running the Ambr15SMMService.msi file. To set up the configuration, open the Ambr® 15 application and navigate to the active experiment if one has already been created for the Ambr® 15 system.

The Ambr® 15 follows a laboratory instrument management system (LIMS)-based configuration to write data to an external source. The LIMS Configuration tab can be accessed through the Configuration section of the Ambr® user interface (Figure 1).

As shown in Figure 1, define a name in the LIMS Configuration and check the Enabled checkbox to allow OPC writability. In the assembly file section, choose the LIMS_OPC_Writer.dll and the class name will be set to LIMS_OPC_Writer by default. Select the OPC Interface XML file if a default configuration is available, or create a new XML file, as shown in Figure 2, and store it in the path C:\AMBR\Configuration\LIMS\.

After completing the settings in Figure 1, define the data refresh interval and assign the configuration variable settings for each culture station and vessel. An Ambr® 15 with 48 culture vessels has four culture stations, each with 12 vessels. Enable all relevant configuration parameters to transmit information to the Kepware® OPC Server. Once the configuration settings are finalized, save the configuration.

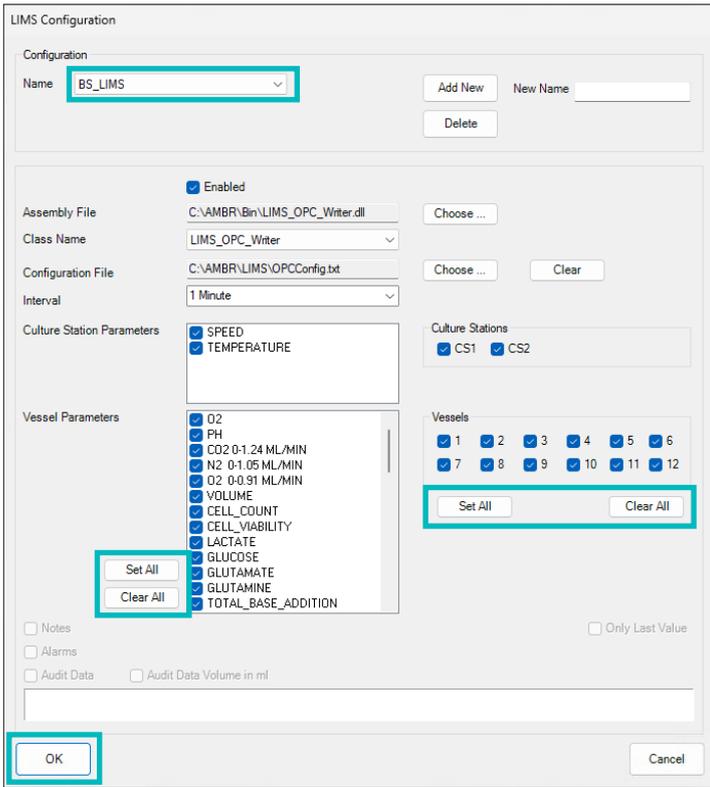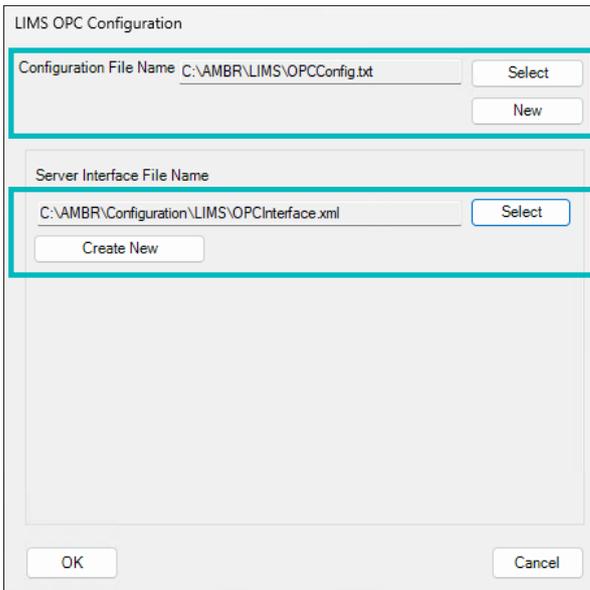**Figure 1:** LIMS Configuration settings in the Ambr® 15 user interface

Figure 2: Creation of an OPC Interface XML configuration file

Step 3: Determination of the OPC UA server endpoint URL
To locate the endpoint URL of the Ambr® 15 system's OPC UA server, right-click the EX icon of the OPC UA Kepware® server (Figure 3) and start the OPC UA Configuration (Figure 4). If a default administrator account was set up during the Kepware® server installation, use those credentials to access the OPC UA Configuration.

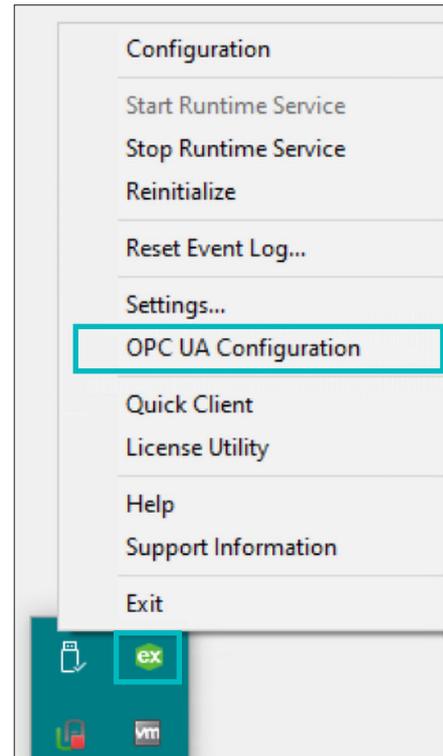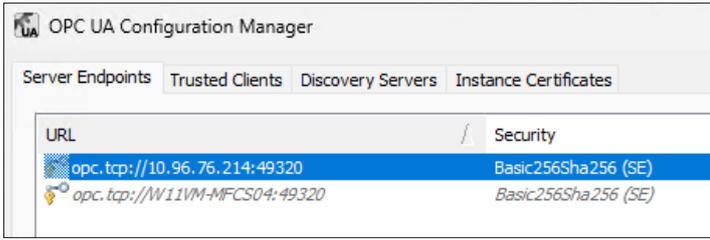**Figure 3:** OPC UA Configuration access through the EX icon
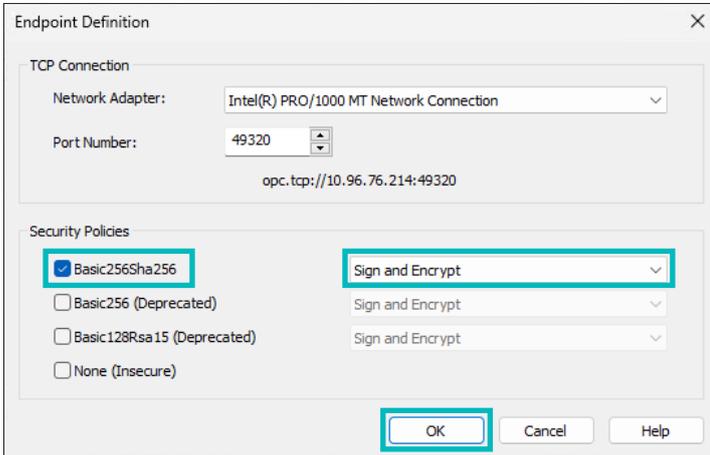
Figure 4: OPC UA server endpoint URL

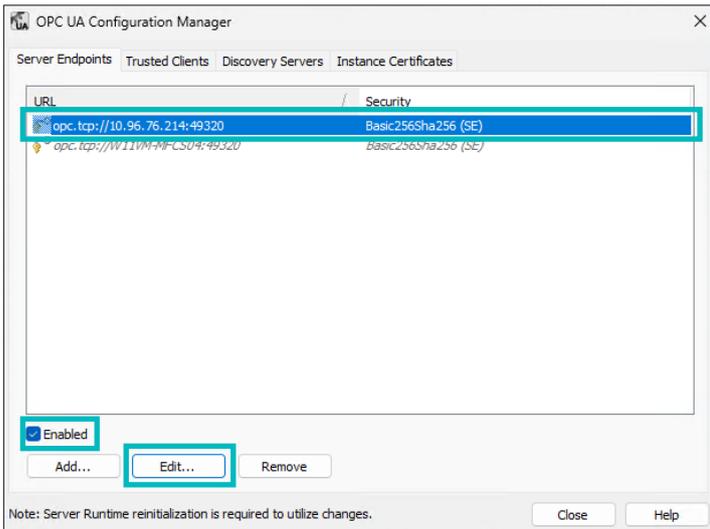Take note of the OPC UA server endpoint URL.

Table 1: OPC UA server endpoint URL of Ambr® 15

URL	opc.tcp://<IP address>:49320
Example	opc.tcp://192.168.138.135:49320

Figure 5: Kepware® OPC UA Configuration Manager: Server Endpoints and Endpoint Definition

Step 4: Configuration of the OPC UA server

Modify the Kepware® OPC UA server configuration using the Kepware® OPC UA Configuration Manager (Figure 5). Select the server URL opc.tcp://<IP Address Biobrain® Supervise Server> and ensure the Enabled setting is checked. Then, press the Edit button and configure the security settings as outlined in Table 2.

To ensure secure client connections to the OPC UA server, apply the most secure profile and disable Anonymous access to prevent unauthorized access. Set the Minimum security mode to Sign and Encrypt to enforce application-level authentication (Figure 5).

Digital signatures ensure message integrity and authenticity, while encryption prevents data from being intercepted by unauthorized parties. The security policy defines the algorithm and key length for signing and encrypting messages. Set the Minimum security policy to Basic256Sha256 and check the Enabled checkbox.

Save changes by clicking the OK button. Table 2 summarizes the default OPC UA server settings that align with these recommendations.

Table 2: Default configuration settings of the Ambr® OPC UA Server

Function	Setting
Security policies none	Deactivated
Minimum security policy	Basic256Sha256
Minimum security mode	Sign and Encrypt
Server	Enabled

Biobrain® Supervise Configuration

Step 1: Configuration of the device connection to the Ambr® system

1. In the DEVICE TYPE-SPECIFIC PROPERTIES tab (Figure 6), configure the TIMING SETTINGS as follows:
   - Polling rate: 5,000 ms
   - Max. retries: 3
   - Reconnect rate: 15 s

Figure 6: General configuration settings of an OPC UA Device in Biobrain® Supervise

2. Under CONNECTION SETTINGS, enter the OPC UA server address (e.g., opc.tcp://<IP address>:49320)

3. Set the Security mode to Sign and Encrypt and the Security policy to Basic256Sha256.

4. Choose Username for the Authentication mode, and enter the username and password for the Kepware® OPC UA server user with Remote operation permissions (e.g., administrator, password: S@rt0r1u5B10t3c).

5. In SECURITY CHECK OVERRIDES, deactivate Accept expired certificates and activate Disable hostname check

These steps are shown in Figure 7.

Figure 7: Device type-specific properties align with the OPC UA server

Table 3 outlines the necessary settings for connecting Biobrain® Supervise to the default configuration of an Ambr® 15 OPC UA server. This configuration tab is also used for the subsequent exchange of OPC UA certificates, described in the following sections.

Table 3: Connection and authentication settings for connecting a Biobrain® Supervise to an Ambr® 15 using default settings

Connection settings

Parameter	Setting
Device address (OPC UA server)	<IP address of Ambr® computer system OPC UA server>:49320
Security mode	Sign and Encrypt
Security policy	Basic256Sha256

Authentication

Parameter	Setting
Username	Administrator
Password	<password for Kepware® user administrator >

Security check overrides

Parameter	Setting
Accept expired certificates	Deactivated
Disable hostname check	Activated

Step 2.1: Certificate exchange and OPC UA connection setup

Upon initial connection between Biobrain® Supervise and the Kepware® OPC UA server, application certificates are exchanged between the Kepware® OPC UA server and the Biobrain® Supervise OPC UA client. Both certificates must be trusted on each side to ensure a secure connection.

Step 2.2: Trusting the server certificate

To initiate the certificate exchange, click the Test connection button in the CONNECTION SETTINGS configuration dialog (Figure 6) of Biobrain® Supervise. The Kepware® OPC UA server will send its application certificate to Biobrain® Supervise, but the connection test will fail because Biobrain® Supervise does not yet trust the server's certificate.

Acknowledge the test result, then open Windows Explorer on the Biobrain® Supervise system and navigate to the folder specified in Table 4. Move the Kepware® OPC UA server's certificate file from the Rejected folder to the Trusted folder (Table 5).

Table 4: Folder locations for rejected and trusted Biobrain® Supervise certificates and file name structure of Kepware® OPC UA server application certificates

Rejected certificates

%ProgramData%\Sartorius\Biobrain_Supervise\Services\OpcUa\Client\pki\rejected\certs

Trusted certificates

%ProgramData%\Sartorius\Biobrain_Supervise\Services\OpcUa\Client\pki\trusted\certs

**Certificate file of the Kepware® OPC UA server**

+KEPServerEX+UA Server+ [<Thumbprint>]. der

Step 2.3: Trusting the Biobrain® Supervise client certificate

Return to Biobrain® Supervise and click Test connection again (Figure 7). The test will fail because the bioreactor's OPC UA server does not yet trust the Biobrain® Supervise client's certificate. Acknowledge the test result.

Next, open the OPC UA Configuration Manager of the Kepware® OPC server (Figure 8). Navigate to the Trusted Clients tab and trust the Biobrain® Supervise client certificate Biobrain_Supervise_OpcClient by clicking the Trust button.

Figure 8: Certificate handling for the Kepware® OPC UA Server.
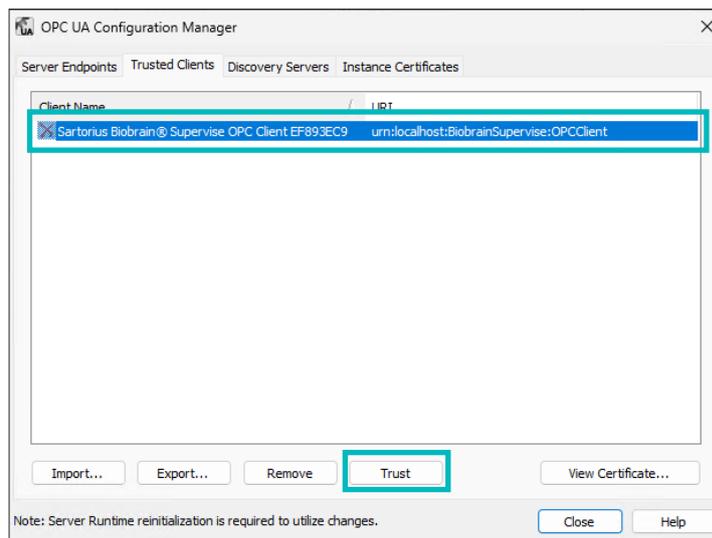
Step 2.4: Verify the correct connection settings

Return to Biobrain® Supervise and click Test connection again (Figure 7). The test will now succeed, as all required application certificates are trusted on both the client and server sides (Figure 8). Acknowledge the test result, proceed with device configuration, and finalize by clicking SAVE to add the new device.

Figure 9: Acknowledgement of the successful connection test in Biobrain® Supervise
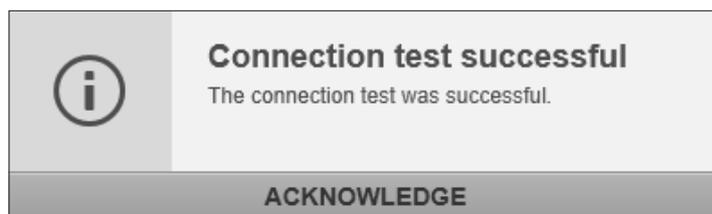
Step 3.1: Configuration of new bioreactor units in Biobrain® Supervise

Create a new unit by selecting ADD UNIT under UNITS in the administration section. In the ADD UNIT dialog, enter a Name (e.g., "Ambr15-CS1") and a Short Name (e.g., "CS1"). Then, click the IMPORT CONTROL MODULES function (Figure 10).
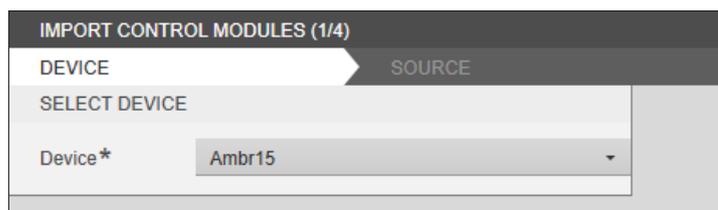
Figure 10: ADD UNIT dialog in Biobrain® Supervise with Import Control Modules functionality highlighted.
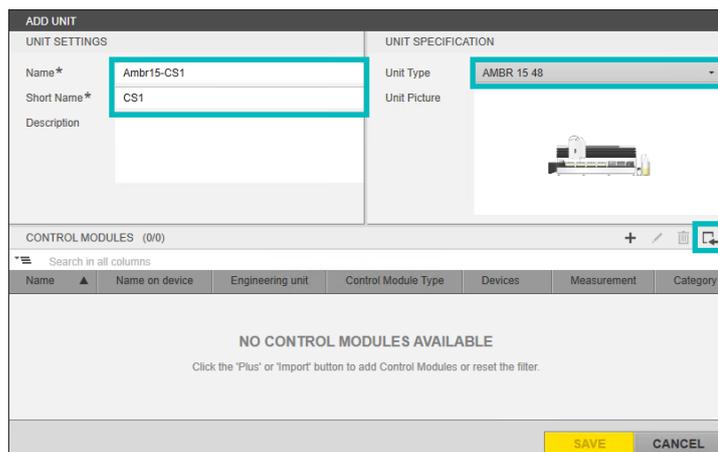

Step 3.2: Importing control modules

In the IMPORT CONTROL MODULES dialog (Figure 11), select the newly created device (e.g., AMBR15), and use NEXT to continue.

Figure 11: Selection of the newly created device

In the file browsing dialog, select and open the factory configuration file for the Ambr® 15, and press NEXT (Figure 12).

Figure 12: Selection of the appropriate configuration file
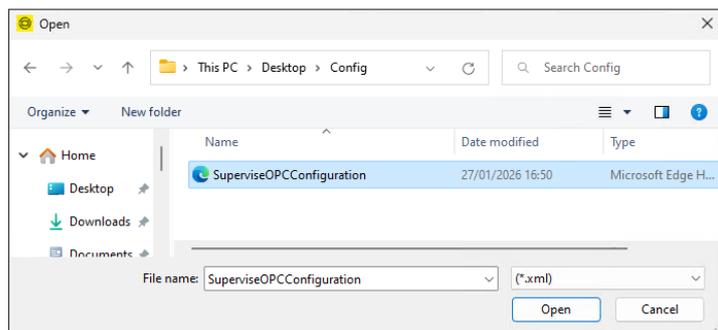
Step 3.3: Selection of the bioreactor from the drop-down list

For the initial run, open the SELECT INSTRUMENT drop-down list (Figure 13) and select Bioreactor 01. In each subsequent run, choose the next bioreactor. Click NEXT after making your selection.
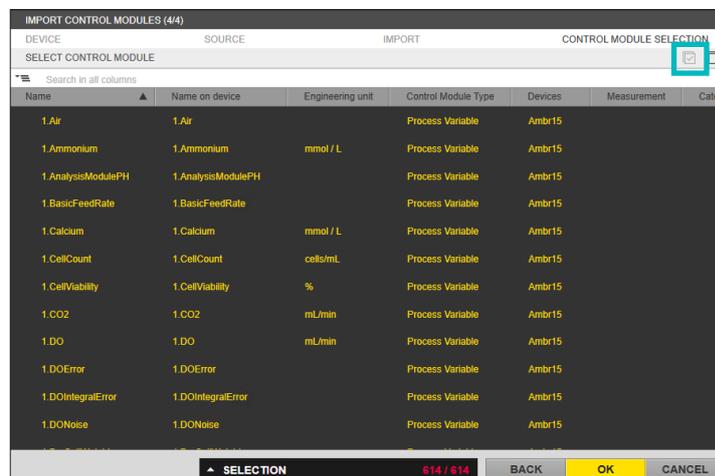
Figure 13: Selection of the appropriate bioreactor from the SELECT INSTRUMENT drop-down list.
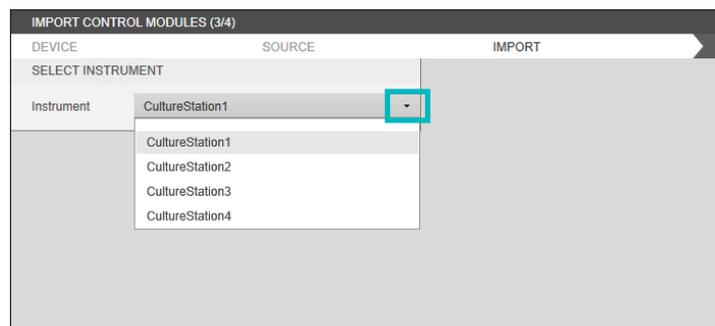
Step 3.4: Selection of all control modules

To select all control modules in the list, press the SELECT ALL CONTROL MODULES button (Figure 14), followed by OK and SAVE.

Figure 14: Selection of all control modules

Repeat steps 3.1–3.4 until all four culture stations of an Ambr® 15 system are created as units. For an Ambr® 15 system with 24 culture vessels and two culture stations, repeat these steps twice.

Following the completion of these steps, a secure connection between Biobrain® Supervise and the Ambr® 15 bioreactor system will be successfully configured and established. Biobrain® Supervise is now ready for supervisory control* and data acquisition of the connected bioreactor.

* Further configuration work on the Ambr® 15 system is required for supervisory control

Conclusion

This application note outlines how to successfully connect bioreactors powered by Ambr® 15 systems with Biobrain® Supervise software via OPC UA to enable convenient supervisory control and data acquisition.

The OPC client functionality of Biobrain® Supervise, utilizing the UA protocol and advanced settings, provides a flexible and secure method for integrating Ambr®-powered bioreactors into Biobrain® Supervise systems using a standardized communication protocol.

As a result, users can enhance a bioreactor system's capabilities with the full range of functionalities provided by Biobrain® Supervise.