OPC UA®

PLC500, PLC500ED, PLC500MC
PLC410

Nota de Aplicación

Nota de Aplicación

PLC410, PLC500, PLC500ED, PLC500MC

Documento: 10013132271

Revisión: 00

Fecha de la Publicación: 04/2025

SUMARIO DE LAS REVISIONES

La informacion abajo describe las revisiones ocurridas en este manual.

Versión	Revisión	Descripción
1.4.2	R00	Primera edición.

SUMARIO

1 INTRODUCCIÓN

Esta Nota de Aplicación está destinada a ayudar en el uso del protocolo **OPC UA®** en los PLCs de WEG, modelos PLC410, PLC500, PLC500ED y PLC500MC. A lo largo de este documento, se utiliza el PLC500 como ejemplo, pero la información presentada es igualmente aplicable a los demás modelos mencionados. Se destaca que los datos proporcionados pueden cambiar ligeramente debido al continuo desarrollo y actualización de los productos y herramientas.

Además de proporcionar una visión general sobre el uso del protocolo OPC UA, este documento presenta las interfaces de comunicación, recomendaciones de instalación, configuraciones de seguridad, ejemplos de topologías de red y una guía para establecer la comunicación OPC UA entre los PLCs y diferentes dispositivos y software, actuando tanto como Servidor como Cliente. Cabe destacar que todos los PLCs WEG con **CODESYS®** incluyen soporte para el Servidor OPC UA. La funcionalidad de Cliente OPC UA está disponible exclusivamente en el PLC500ED, mediante programación en la plataforma WEGnology.

Para más información sobre el hardware, interfaces y protocolos de comunicación, consulte el Manual del Usuario del producto correspondiente, disponible en el sitio web de WEG. Para una descripción más profunda y detallada sobre OPC UA, acceda a la ayuda en línea en CODESYS Online Help.

¡ATENCIÓN!

Esta nota de aplicación está dirigida a profesionales capacitados en redes industriales. La instalación y configuración de los dispositivos debe realizarse de acuerdo con el manual del fabricante.

¡NOTA!

Se recomienda utilizar **CODESYS** versión **V3.5 SP19** o superior, así como la versión más reciente de las bibliotecas de configuración para OPC UA.

1.1 ABREVIACIONES Y DEFINICIONES UTILIZADAS

CA: Entidad pública o privada que forma parte de la cadena de confianza de la certificación digital, responsable de emitir, revocar y renovar certificados digitales *(Certificate Authority)*.

CODESYS: Plataforma de programación que permite desarrollar, configurar y monitorear soluciones para automatización industrial e integración de sistemas.

Edge Agent: Contenedor previamente instalado en el PLC500ED que permite la ejecución local de Edge Workflows.

IoT: Sigla que se refiere a las tecnologías que facilitan la comunicación y el intercambio de datos entre dispositivos y la nube, así como entre los propios dispositivos (*Internet of Things*).

IIoT: Aplicación de tecnologías IoT en el contexto industrial, conectando dispositivos, máquinas y sistemas a través de Internet para la recolección, intercambio y análisis de datos, con el objetivo de mayor eficiencia, automatización y monitoreo *(Industrial Internet of Things)*.

OPC UA: Protocolo de comunicación industrial que garantiza interoperabilidad segura entre dispositivos y sistemas. Ofrece criptografía, autenticación y soporte para modelos de datos complejos, siendo ampliamente utilizado en automatización e IIoT (*Open Platform Communications Unified Architecture*).

SCADA: Sistema que monitorea y controla procesos industriales en tiempo real, recolectando datos de sensores y dispositivos locales y remotos para análisis y operación centralizada (*Supervisory Control and Data Acquisition*).

UAExpert: Software utilizado como un Cliente OPC UA de prueba de uso general, soportando recursos como *DataAccess*, *Alarms* & *Conditions*, Acceso Histórico y llamada de Métodos UA.

WEGnology: Plataforma IIoT de WEG para monitoreo, análisis y automatización de procesos industriales, permitiendo la conexión de dispositivos y la gestión de datos en tiempo real.

WES: WEGnology Edge Suite es un software moderno y avanzado para supervisión, control y automatización de procesos industriales y desarrollo de aplicaciones Edge IoT.

1.2 EL PROTOCOLO OPC UA

El OPC UA (*Open Platform Communications Unified Architecture*) es un protocolo de comunicación industrial independiente de plataforma que garantiza interoperabilidad segura y confiable entre dispositivos, máquinas y sistemas de diferentes fabricantes. Desarrollado y mantenido por la **OPC Foundation**, fue diseñado para reemplazar versiones anteriores del OPC, ofreciendo soporte para modelos de información complejos y seguridad avanzada, incluyendo criptografía y autenticación.

El estándar OPC es una serie de especificaciones desarrolladas por proveedores de la industria, usuarios finales y desarrolladores de software. Estas especificaciones definen la interfaz entre Clientes y Servidores, incluyendo acceso a datos en tiempo real, monitoreo de alarmas y eventos. Ampliamente utilizado en automatización industrial, SCADA, IIoT e integración de sistemas, el OPC UA estandariza el intercambio de datos en diversos entornos.

En **CODESYS**, el OPC UA está integrado como Servidor nativo, permitiendo que Clientes OPC UA accedan a variables del dispositivo de forma estructurada y segura. La configuración se realiza en **Symbol Configuration**, donde los datos compartidos pueden tener control de acceso de lectura y escritura. Con soporte para criptografía y autenticación, este protocolo facilita la comunicación entre PLCs y sistemas industriales. Para más detalles, consulte la documentación oficial en el sitio web de CODESYS y de la OPC Foundation.

1.3 DOCUMENTOS DE REFERENCIA

Se recomienda consultar los documentos relacionados con OPC UA mostrados en la Tabla 1.1 en la pagina 1-2.

Tabla 1.1: *Documentos de referencia.*

Documento	Versión	Fuente
Practical Security Recommendations for building OPC UA Applications	3	OPC Foundation

1.4 AVISO IMPORTANTE SOBRE SEGURIDAD CIBERNÉTICA Y COMUNICACIONES

Los PLCs de WEG, modelos PLC410, PLC500, PLC500ED y PLC500MC, tienen la capacidad de conectarse e intercambiar información a través de redes y protocolos de comunicación. Aunque han sido diseñados y probados para garantizar el funcionamiento adecuado con otros sistemas de automatización utilizando los protocolos mencionados en este manual, es esencial que el cliente comprenda las responsabilidades asociadas a la información y la ciberseguridad al utilizar este equipo.

Por lo tanto, es responsabilidad del cliente adoptar estrategias de defensa en profundidad e implementar políticas y medidas para garantizar la seguridad del sistema en su totalidad, incluyendo las comunicaciones enviadas y recibidas por el equipo. Estas medidas incluyen, pero no se limitan a, instalación de firewalls, programas antivirus y antimalware, cifrado de datos, control de autenticación y control físico de acceso de los usuarios.

WEG y sus afiliadas no se responsabilizan por daños o pérdidas derivados de violaciones de seguridad cibernética, incluyendo, pero no limitándose a, acceso no autorizado, intrusión, fuga y/o robo de datos o información, denegación de servicio o cualquier otra forma de violación de seguridad. El uso de este producto en condiciones para las cuales no fue específicamente diseñado no es recomendado y puede causar daños al producto, a la red y al sistema de automatización.

En este sentido, es imprescindible que el cliente comprenda que intervenciones externas mediante programas de terceros, como los sniffers o programas con acciones similares, tienen el potencial de ocasionar interrupciones o restricciones en la funcionalidad del equipo.

1.5 MARCAS REGISTRADAS

OPC UA® es una marca registrada de OPC Foundation.

Todas las demás marcas registradas son propiedad de sus respectivos titulares.

2 INTERFAZ ETHERNET

La comunicación OPC UA se realiza a través de las conexiones Ethernet, indicadas en la Figura 2.1 en la pagina 2-1 para el PLC500 y PLC410. Inicialmente, cada puerto Ethernet tiene la dirección IP indicada en la Tabla 2.1 en la pagina 2-1, que puede ser modificada en cualquier momento a través del software CODESYS.

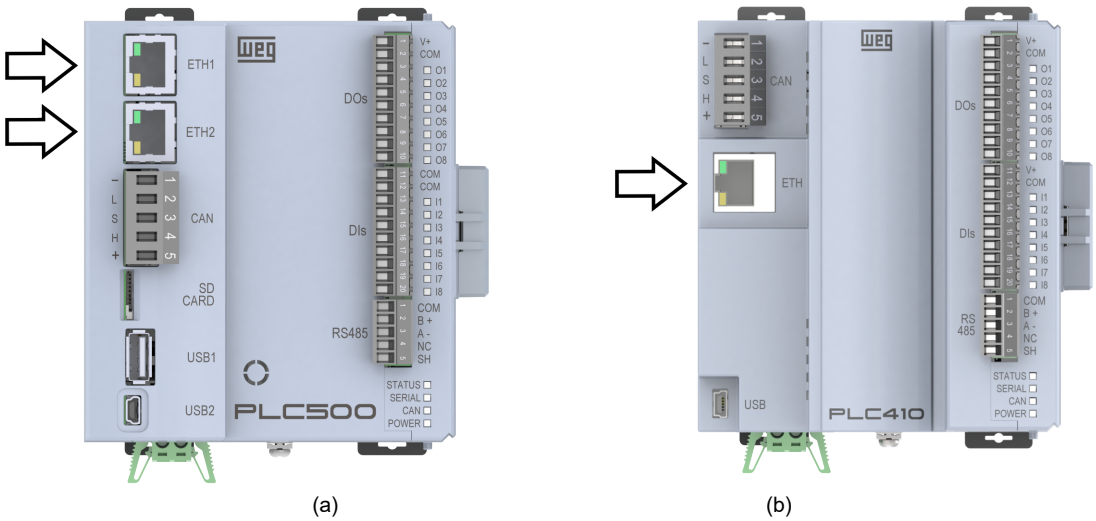


Figura 2.1: *Indicación de las conexiones Ethernet de los PLCs. (a) PLC500 y (b) PLC410.*

Tabla 2.1: *Direcciones predeterminadas para los puertos Ethernet.*

PLC410	PLC500	Dirección IP predeterminada
ETH	ETH1	192.168.1.10
-	ETH2	192.168.2.10

La distribución de los pines del conector sigue el estándar Ethernet 1000BASE-TX. La interfaz Ethernet del PLC410 soporta velocidades de hasta 100 Mbps, mientras que las interfaces Ethernet del PLC500 alcanzan hasta 1000 Mbps.

Los PLCs PLC500, PLC500ED y PLC500MC tienen dos interfaces Ethernet, que pueden configurarse en modo **Independent**, en el cual las interfaces operan con IPs distintos, o en modo **Switch**, donde las interfaces comparten la misma dirección IP.

Las interfaces Ethernet son compatibles con varios protocolos de comunicación, incluyendo OPC UA, y pueden utilizarse simultáneamente para múltiples protocolos. Para instrucciones sobre cómo configurar estas redes adicionales, consulte las Notas de Aplicación del producto disponibles en el sitio web de WEG.

2.1 LEDS DE INDICACIÓN

Los puertos Ethernet tienen LEDs para indicar la velocidad y el enlace/actividad de la red, como se indica en la Figura 2.2 en la pagina 2-2. Estos LEDs tienen el comportamiento descrito en la Tabla 2.2 en la pagina 2-2 y la Tabla 2.3 en la pagina 2-2.

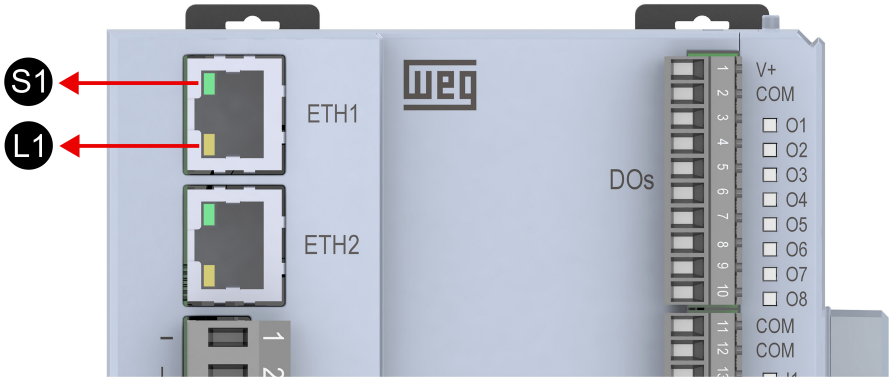


Figura 2.2: *LEDs de velocidad (S1) y enlace/actividad (L1) de la interfaz Ethernet del PLC500.*

Tabla 2.2: *LED S1 - Velocidad.*

Estado	Descripción
Apagado	Equipo apagado o enlace de 10 Mbps
Verde, sólido	Enlace de 100 Mbps

Tabla 2.3: *LED L1 - Enlace/Actividad.*

Estado	Descripción
Apagado	Equipo apagado o sin enlace
Ámbar, sólido	Con enlace y sin actividad en la red
Ámbar, parpadeando	Con enlace y con actividad en la red

2.2 INSTALACIÓN DE LA RED OPC UA

La red OPC UA, como varias redes de comunicación industriales, debido a que se aplica muchas veces en ambientes agresivos y con alta exposición a la interferencia electromagnética, exige ciertos cuidados que deben tomarse para garantizar una baja tasa de errores de comunicación durante su operación.

¡ATENCIÓN!

Se recomienda el uso de componentes pasivos (cables, conectores, switches, hubs) certificados para aplicaciones industriales.

Las características recomendadas para el cable utilizado en la instalación son:

- Cable estándar Ethernet, 1000Base-TX, CAT 5e o superior.
- Cable blindado.
- Longitud máxima de 100 m para conexión entre equipos.

Una conexión adecuada al sistema de puesta a tierra es esencial para minimizar problemas de interferencia electromagnética en ambientes industriales. Es importante evitar la conexión del cable en múltiples puntos de puesta a tierra, especialmente en lugares donde hay diferencias de potencial entre los puntos de tierra. Además, se recomienda que los cables de señal y comunicación se instalen en rutas dedicadas, manteniendo distancia de los cables de potencia.

¡PELIGRO!

Instalaciones de puesta a tierra inadecuadas pueden causar fallos en la red OPC UA y representar riesgo de choque eléctrico fatal.

2.3 TOPOLOGÍAS DE RED OPC UA

Las topologías de red en un sistema OPC UA pueden variar según las necesidades del proyecto y la arquitectura de la instalación. En la Figura 2.3 en la pagina 2-3 se muestra un ejemplo de topología en estrella, en la cual un switch central conecta todos los dispositivos clientes y servidores OPC UA.

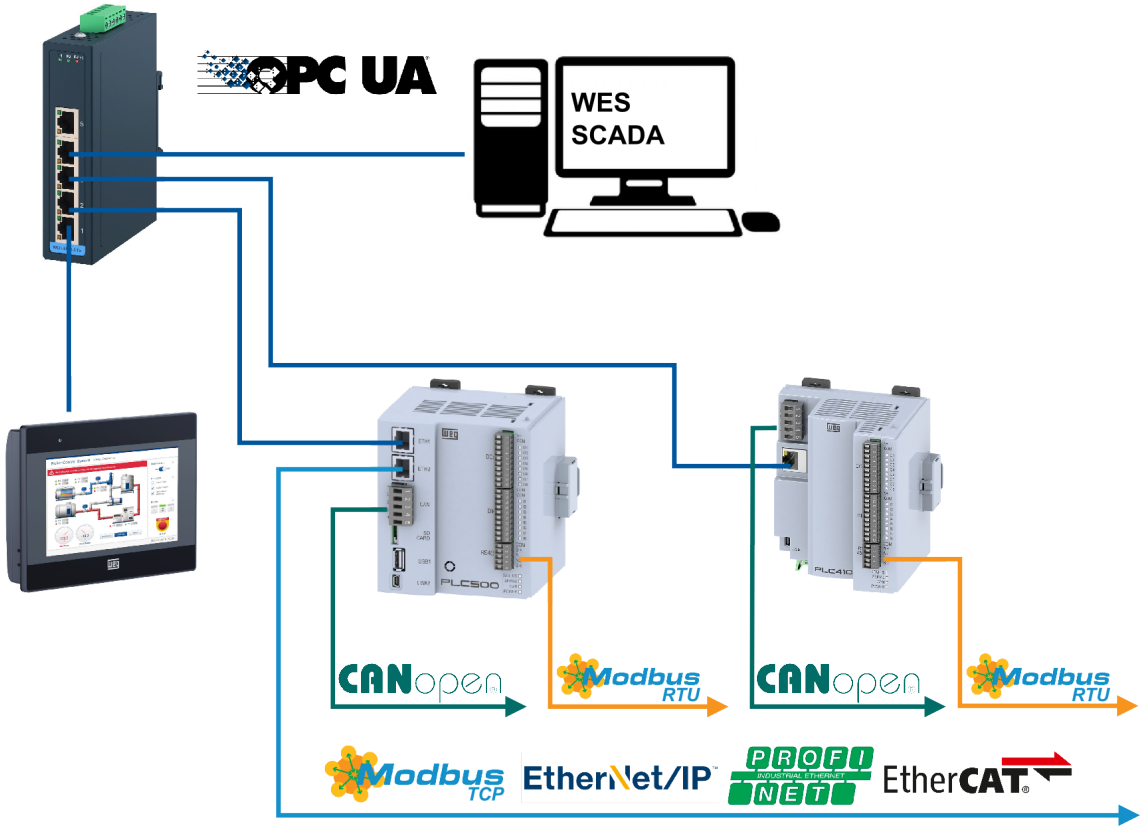


Figura 2.3: *Ejemplo de topología de red OPC UA integrada a otros protocolos de comunicación utilizados en ambientes industriales.*

En la figura, la IHM puede actuar como Servidor OPC UA para un sistema SCADA, como el WES ejecutándose en una computadora, al mismo tiempo que se comporta como Cliente de los PLCs PLC500 y PLC410. Además, es posible establecer comunicación directa entre los PLCs, donde uno puede configurarse como Servidor y el otro como Cliente OPC UA, permitiendo el intercambio de datos de forma estructurada.

Para control y monitoreo de dispositivos industriales, tanto el PLC500 como el PLC410 soportan varios protocolos de comunicación, incluyendo CANopen, Modbus RTU, Modbus TCP, EtherNet/IP, PROFINET y EtherCAT, garantizando integración con una amplia gama de equipos y redes industriales. Esta flexibilidad posibilita desde la comunicación con sensores y actuadores hasta la interconexión con sistemas avanzados de supervisión y control distribuido.

¡NOTA!

Para más información sobre los protocolos de comunicación del PLC500 y PLC410, consulte las Notas de Aplicación disponibles en sus respectivas páginas de producto en el sitio web de WEG.

3 CONFIGURACIONES DE SEGURIDAD

En esta sección, se detallan las opciones de seguridad para la comunicación OPC UA del PLC500 en CODESYS. Las configuraciones pueden ajustarse según los requisitos de cada aplicación, sin embargo, se recomienda siempre utilizar el nivel más alto de seguridad disponible.

3.1 CODESYS SECURITY AGENT

El complemento **CODESYS Security Agent** permite configurar y gestionar aspectos esenciales de seguridad en el entorno de desarrollo CODESYS. En las versiones más recientes, ya viene preinstalado. Si no está disponible en su sistema, siga los pasos a continuación para instalarlo.

Para instalar el complemento, acceda a **Tools** → **CODESYS Installer**. En la nueva ventana abierta, haga clic en **Browse** y busque **Security**. Luego, seleccione **CODESYS Security Agent** y haga clic en **Install**, como se ilustra en la Figura 3.1 en la pagina 3-1. Antes de instalar nuevos complementos a través de CODESYS Installer, asegúrese de que el software CODESYS esté cerrado.

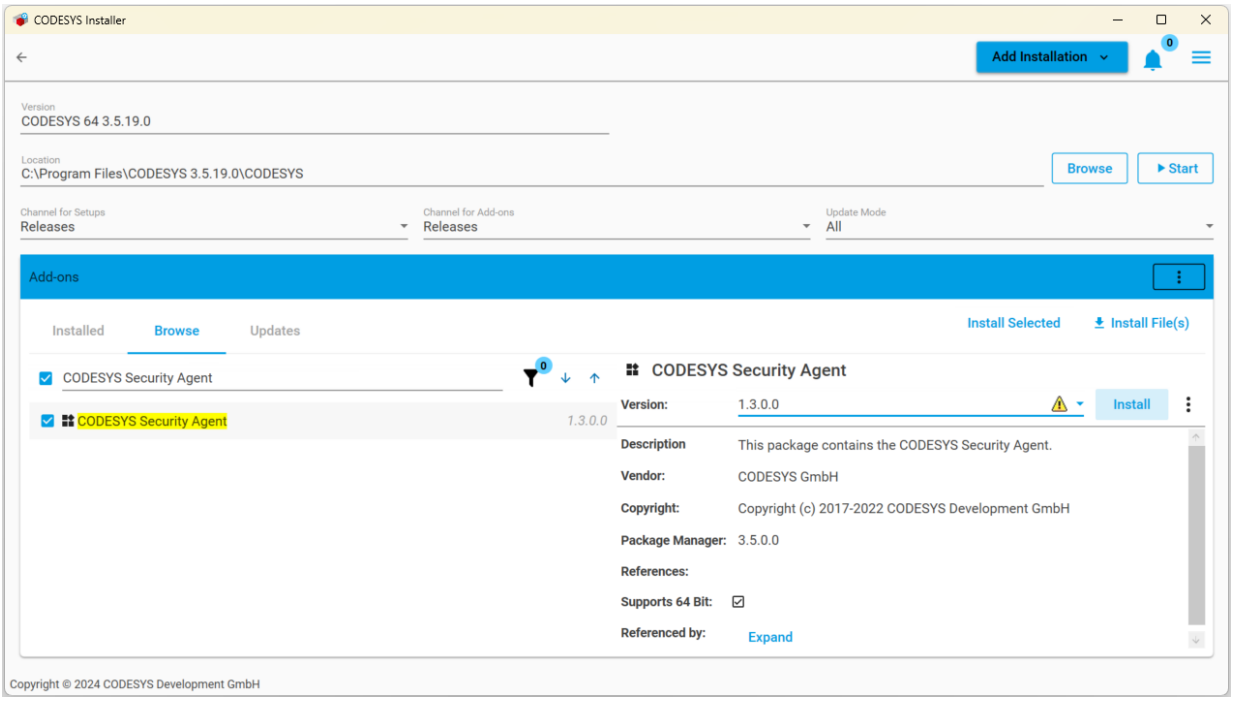


Figura 3.1: *Instalando el complemento CODESYS Security Agent.*

3.2 RUNTIME CODESYS

Las configuraciones de seguridad del runtime de CODESYS pueden modificarse accediendo a **Communication Settings** → **Device** → **Change Runtime Security Policy**, como se ilustra en la Figura 3.2 en la pagina 3-2.

En la sección **Device User Management**, es posible definir la gestión de inicio de sesión del usuario como opcional (**Optional user management**) u obligatoria (**Enforce user management**). Además, la opción **Allow anonymous login** permite establecer una conexión OPC UA sin la necesidad de proporcionar credenciales de usuario y contraseña.

NOTA DE CIBERSEGURIDAD!

Se recomienda no permitir conexiones anónimas vía OPC UA, ya que esto puede exponer el sistema a accesos no autorizados y vulnerabilidades de seguridad. La OPC Foundation sugiere que la autenticación se realice mediante inicio de sesión con usuario y contraseña (**Sign**) o con autenticación y cifrado (**SignAndEncrypt**).

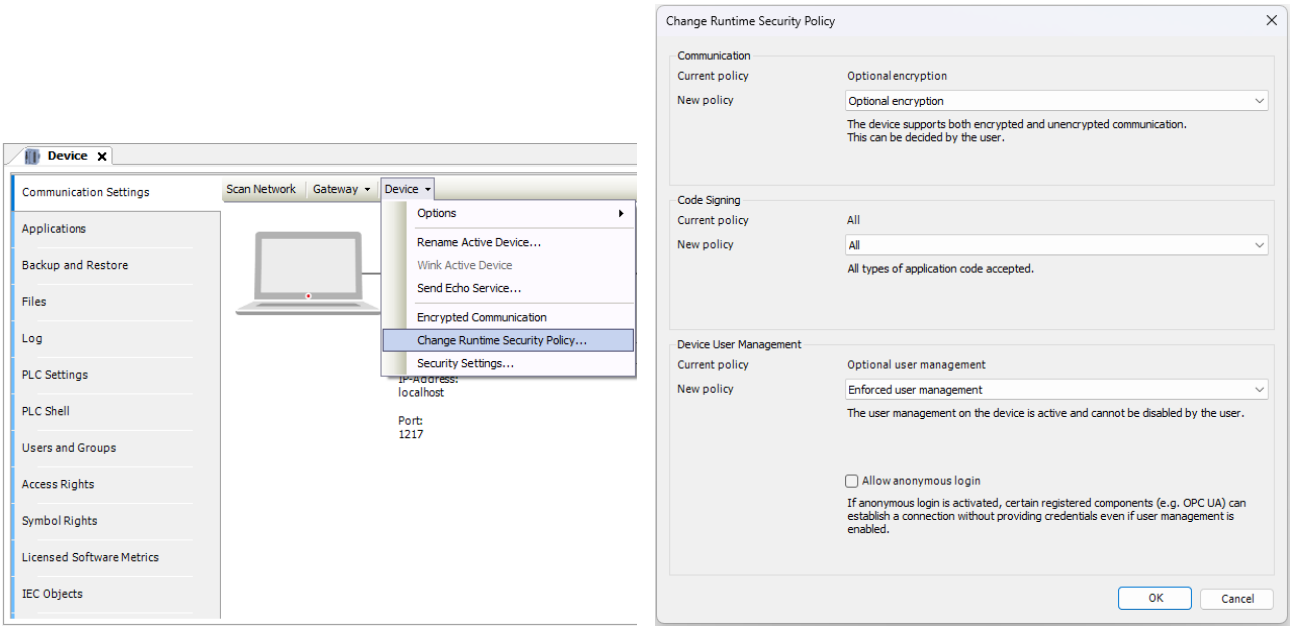


Figura 3.2: *Accediendo a configuraciones de seguridad del runtime de CODESYS.*

NOTA DE CIBERSEGURIDAD!

CODESYS ofrece diversas funcionalidades de seguridad, incluyendo cifrado en la comunicación entre el runtime y el PLC, control de acceso a la aplicación por usuarios, autenticación basada en certificados, protección contra manipulación de código fuente, firmas digitales para aplicaciones, entre otras. Estas medidas garantizan mayor protección contra accesos no autorizados y manipulaciones indebidas. Para más información, consulte la ayuda en línea en CODESYS Online Help.

Si la opción **Enforce user management** está habilitada, será necesario proporcionar credenciales para establecer la conexión del Cliente con el Servidor OPC UA. Si ningún usuario está configurado en el PLC, en el próximo intento de inicio de sesión, el sistema solicitará la creación de un nuevo usuario y contraseña, como se ilustra en la Figura 3.3 en la pagina 3-2.

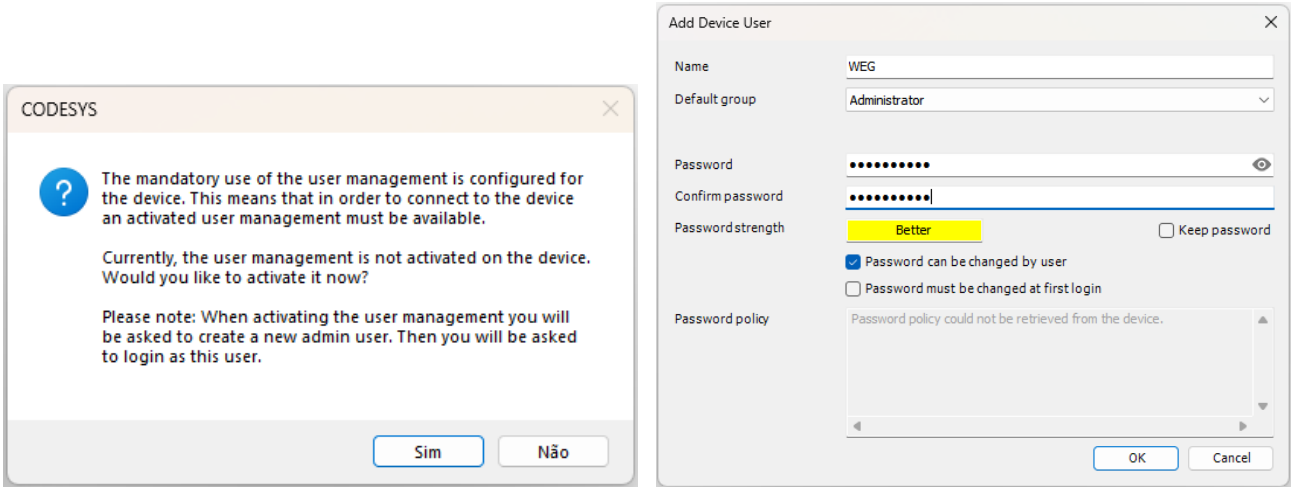


Figura 3.3: *Configuración obligatoria de usuario para iniciar sesión en el PLC.*

NOTA DE CIBERSEGURIDAD!

Siempre utilice contraseñas fuertes al iniciar sesión en el PLC, combinando letras mayúsculas y minúsculas, números y caracteres especiales. Durante la puesta en marcha, cambie cualquier contraseña predeterminada existente y establezca una política de cambios regulares para reforzar la seguridad del sistema.

Si el usuario y/o la contraseña para iniciar sesión en el PLC se olvidan, el acceso al dispositivo puede recuperarse mediante el **Factory Reset**, que restaura las configuraciones de fábrica del producto. Esta funcionalidad está disponible a través de la página web, del PLC Shell en CODESYS y también a través de SmartMedia. Para más detalles, consulte los manuales de los productos, disponibles en el sitio web de WEG.

¡ATENCIÓN!

Al realizar la restauración de los datos de fábrica, **todas las aplicaciones de CODESYS, registros, archivos almacenados en el PLC y configuraciones de red serán eliminados**. El producto se reiniciará automáticamente después de la conclusión de estas operaciones.

3.3 CONFIGURACIONES DE SEGURIDAD DEL OPC UA

Las configuraciones de seguridad del Servidor OPC UA pueden visualizarse en **Communication Settings** → **Device** → **Security Settings**, como muestra la Figura 3.4 en la pagina 3-3. En esta ventana, se puede modificar la política de seguridad utilizada para la autenticación de la comunicación entre el Cliente y el Servidor OPC UA.

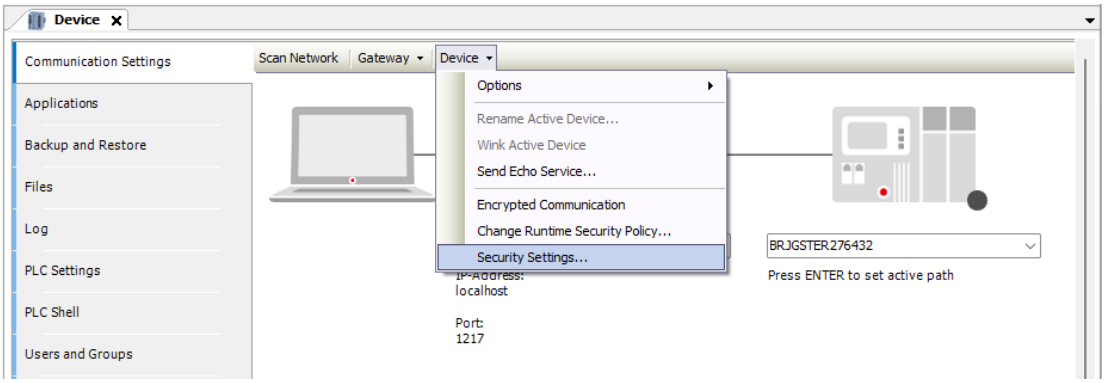


Figura 3.4: *Accediendo a las configuraciones de seguridad del PLC500.*

A través del ícono **+** en **CmpOPCUAServer**, se tienen las posibles configuraciones de seguridad e información del Servidor OPC UA, de acuerdo con la Figura 3.5 en la pagina 3-3.

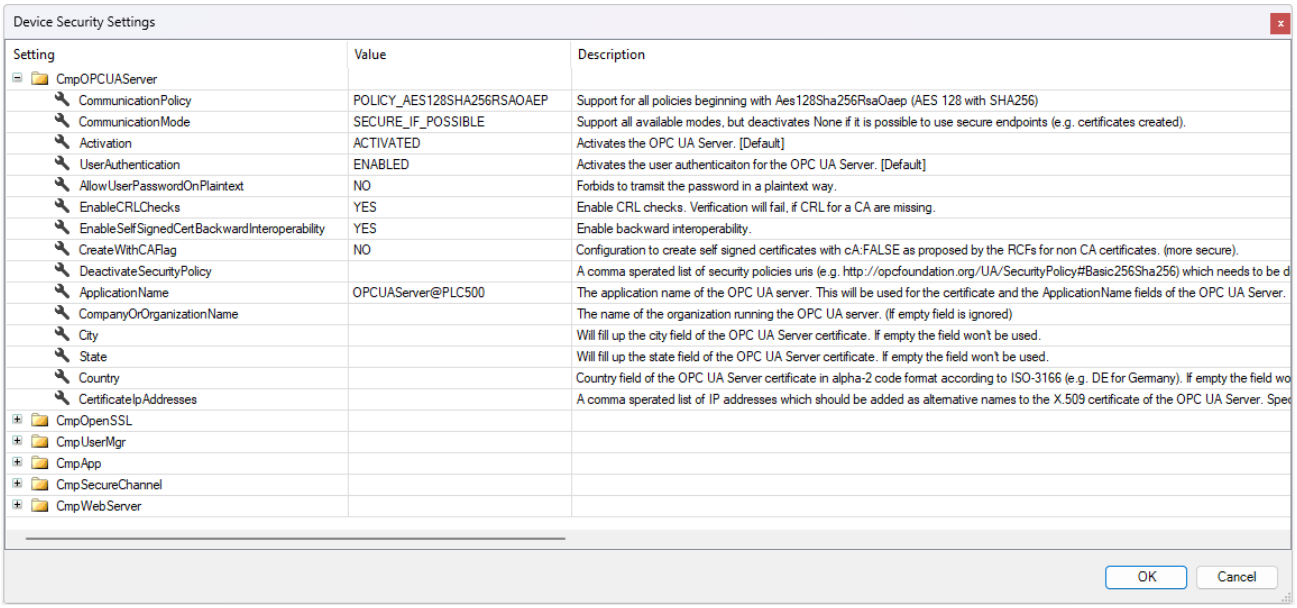


Figura 3.5: *Configuraciones de seguridad del Servidor OPC UA.*

El campo **CommunicationPolicy** define la política de seguridad soportada por el Servidor OPC UA. Las políticas disponibles son: Aes256Sha256RsaPss, Basic256Sha256 y Aes128Sha256RsaOaep. La OPC Foundation recomienda la utilización, como mínimo, de la política Basic256Sha256. Algoritmos de cifrado obsoletos, que utilizan SHA-1, no deben emplearse.

En **CommunicationMode**, es posible configurar el modo de conexión permitido por el Servidor OPC UA. Se recomienda utilizar la opción MIN_SIGNED, la cual exige siempre usuario y contraseña.

¡NOTA!

Para romper un cifrado AES-128 por fuerza bruta, serían necesarias 2^{128} combinaciones. Con una supercomputadora capaz de realizar 1×10^{18} operaciones por segundo, el tiempo estimado para la tarea sería de hasta $10,8 \times 10^{12}$ (billones) de años.

Para más información sobre las opciones de seguridad del OPC UA, consulte la ayuda en línea en CODESYS Online Help.

3.4 CREACIÓN DE CERTIFICADO AUTOFIRMADO

Para crear un certificado autofirmado, acceda a **View** → **Security Screen** o haga clic en el ícono, ubicado en la esquina inferior izquierda de la ventana de CODESYS, como se ilustra en la Figura 3.6 en la pagina 3-4.

En la ventana que se abrirá, seleccione la pestaña **Devices**, haga clic en el ícono de actualización y, a continuación, haga clic en el ícono **Device** para visualizar los certificados disponibles, como se muestra en la Figura 3.7 en la pagina 3-4.

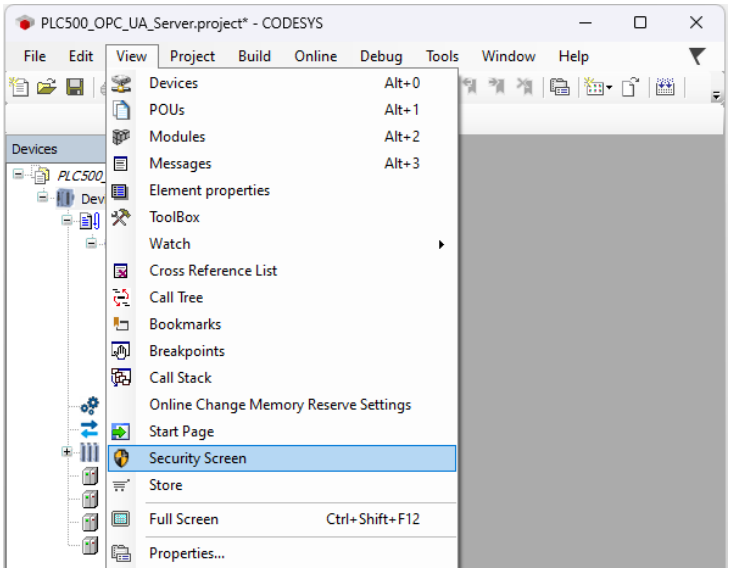


Figura 3.6: *Apertura de la pantalla de seguridad en CODESYS.*

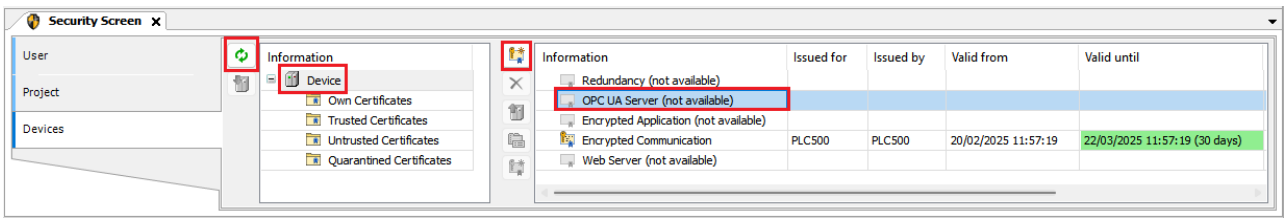


Figura 3.7: *Pantalla de certificados del dispositivo.*

Para crear un nuevo certificado, acceda a **OPC UA Server** y haga clic en el ícono. A continuación, elija el tamaño de la clave, defina la validez del certificado y haga clic en **OK**.

Espere la generación del certificado — cuanto mayor sea el tamaño de la clave, más seguro será el certificado, pero el proceso de creación llevará más tiempo. Después de la conclusión, el certificado podrá visualizarse como se ilustra en la Figura 3.8 en la pagina 3-5. Además, los certificados creados por el PLC500 pueden listarse directamente a través de PLC Shell, utilizando el comando **cert-getcertlist**.

¡NOTA!

El certificado utilizado para el cifrado de la comunicación entre CODESYS en la computadora y el PLC se genera automáticamente, sin necesidad de creación manual.

Information	Issued for	Issued by	Valid from	Valid until
Redundancy (not available)				
OPC UA Server	OPCUAServer@PLC500	OPCUAServer@PLC500	20/02/2025 12:01:15	22/03/2025 12:01:15 (30 days)
Encrypted Application (not available)				
Encrypted Communication	PLC500	PLC500	20/02/2025 11:57:19	22/03/2025 11:57:19 (30 days)
Web Server (not available)				

Figura 3.8: *Nuevo certificado Servidor OPC UA generado en CODESYS.*

NOTA DE CIBERSEGURIDAD!

Los certificados generados por CODESYS no tienen la autenticidad de una Autoridad Certificadora (CA), por lo tanto, cualquier Cliente OPC UA que desee realizar una comunicación segura debe reconocer manualmente el certificado generado.

4 SERVIDOR OPC UA - CODESYS

Esta sección presenta un ejemplo de configuración de un Servidor OPC UA en CODESYS utilizando el PLC500.

Inicialmente, agregue la **Symbol Configuration** a la aplicación: haga clic con el botón derecho en **Application** → **Add Object** → **Symbol Configuration**, como se ilustra en la Figura 4.1 en la pagina 4-1. Marque la opción **Support OPC UA features option** y haga clic en **Add**.

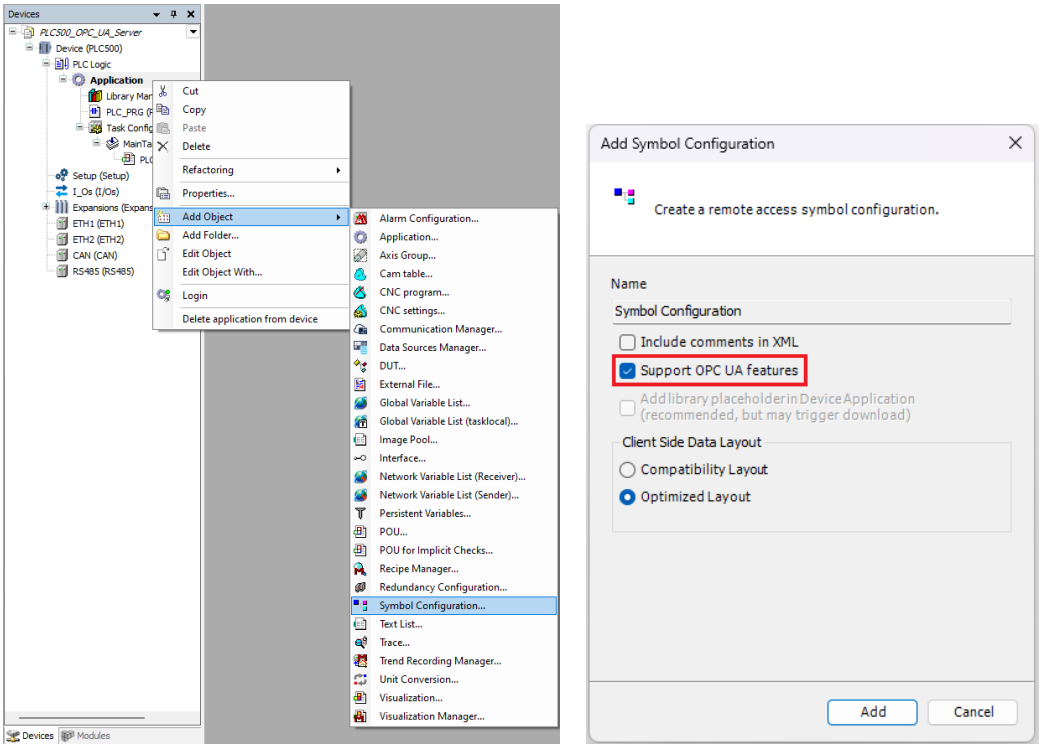


Figura 4.1: *Agregando la Symbol Configuration a la aplicación en CODESYS y habilitando las funciones OPC UA.*

A continuación, en **Symbol Configuration**, haga clic en **Build**. Los símbolos se crearán para todas las variables declaradas en el proyecto. Para seleccionar los datos que se pondrán a disposición del Servidor OPC UA, habilite las casillas ☑ haciendo clic con el botón izquierdo en la lista de **Symbols**, como se muestra en la Figura 4.2 en la pagina 4-1.

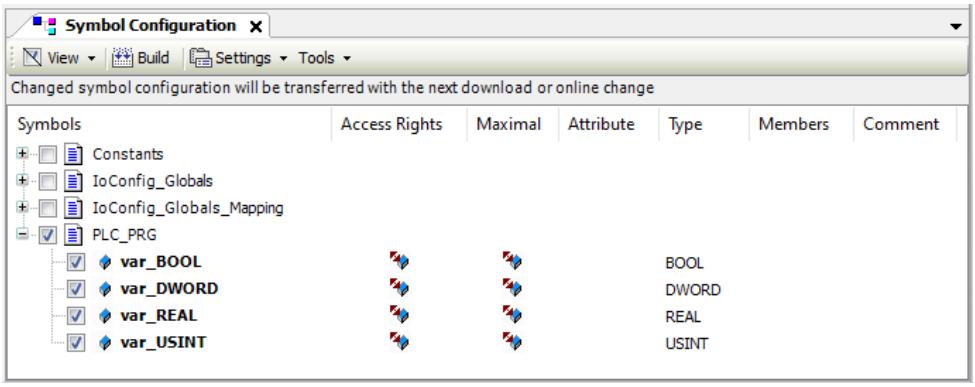


Figura 4.2: *Configuración de variables en Symbol Configuration.*

¡NOTA!

Por defecto, las variables tienen derechos de acceso para lectura y escritura por el Cliente OPC UA, como se observa en la variable **var_DWORD**, indicada por el ícono . Las variables con acceso solo de lectura tienen el ícono , mientras que aquellas con acceso solo de escritura tienen el ícono . Para modificar el tipo de acceso, haga clic con el botón izquierdo sobre los íconos.

5 CLIENTE OPC UA - UA EXPERT

Esta sección presenta un ejemplo de configuración de un Cliente OPC UA en **UAExpert®**. El programa está disponible para descarga en el sitio web de Unified Automation.

5.1 ENCONTRANDO SERVIDORES POR URL

En UAExpert, haga clic en el ícono **+** para agregar un Servidor OPC UA. Luego, haga doble clic en el **+** de **Custom Discovery** y escriba la URL correspondiente a la IP de su Servidor OPC UA. Por ejemplo, si la IP es 192.168.1.10, la URL será **opc.tcp://192.168.1.10:4840**. La Figura 5.1 en la pagina 5-1 muestra los pasos para agregar el Servidor OPC UA en UAExpert.

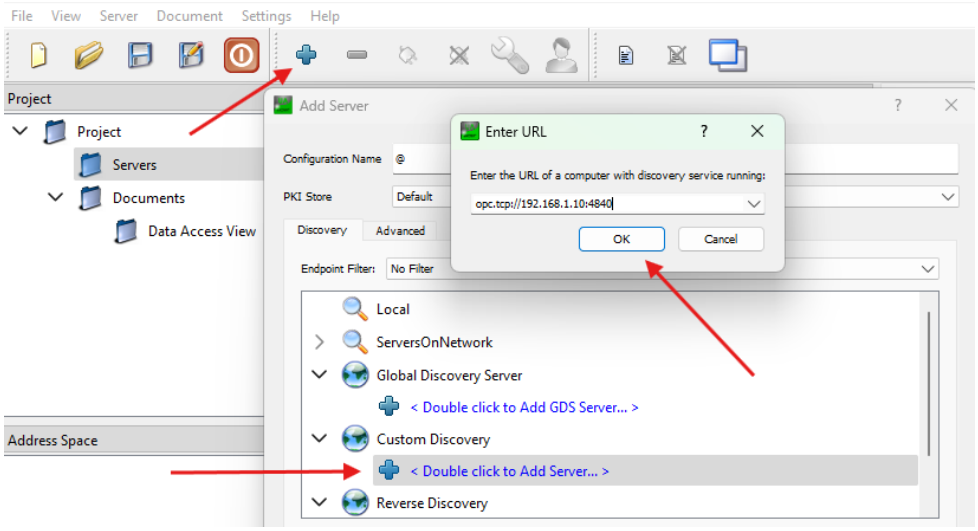


Figura 5.1: *Adición del Servidor OPC UA en UAExpert.*

A continuación, haga clic en la URL y expanda los íconos hasta que se muestren las conexiones disponibles. Dependiendo de la configuración de seguridad del Servidor OPC UA del PLC500, no todas las opciones estarán visibles. Utilice las opciones de conexión que presenten un Endpoint URL con la dirección IP del Servidor OPC UA del PLC500, como se muestra en la Figura 5.2 en la pagina 5-1. Los Endpoint URL con el nombre del host generarán un error de conexión.

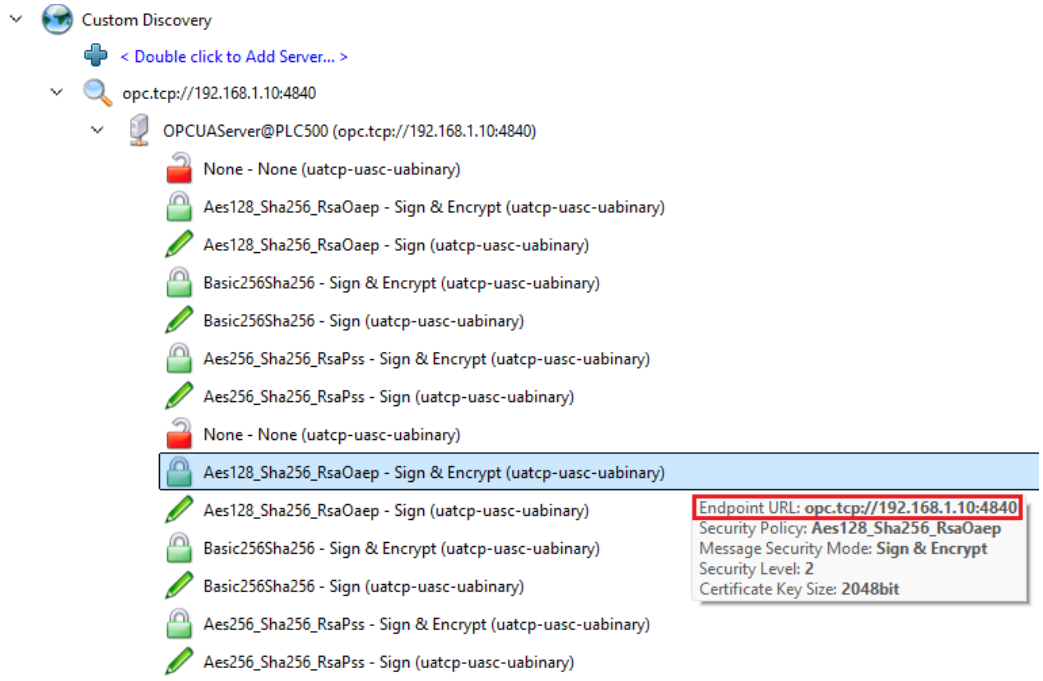


Figura 5.2: *Todas las opciones de conexión del Servidor OPC UA del PLC500 en UAExpert.*

¡NOTA!

Para que todas las opciones de conexión aparezcan en UAExpert, se debe crear un certificado autofirmado para OPC UA en el PLC500. Además, el **CommunicationMode** debe estar configurado en **ALL**. Consulte la Sección 3 CONFIGURACIONES DE SEGURIDAD en la pagina 3-1 para más información.

5.2 CONEXIÓN ANÓNIMA

Para que una conexión anónima sea posible, es necesario habilitar la opción **Allow anonymous login** en **Change Runtime Security Policy** y configurar **CommunicationMode** en **ALL** en **Device Security Settings**.

NOTA DE CIBERSEGURIDAD!

El uso de conexión anónima para la operación regular de aplicaciones no se recomienda debido a cuestiones de ciberseguridad. Debe restringirse a fines de prueba, puesta en marcha o cuando no haya otras alternativas disponibles.

Seleccione la opción de conexión **None** y haga clic en **OK**, como se muestra en la Figura 5.3 en la pagina 5-2. El Servidor OPC UA aparecerá debajo de la carpeta **Servers**. Haga clic con el botón derecho y seleccione **Connect**, o haga clic en el ícono correspondiente en la barra de herramientas, como se muestra en la Figura 5.4 en la pagina 5-2.

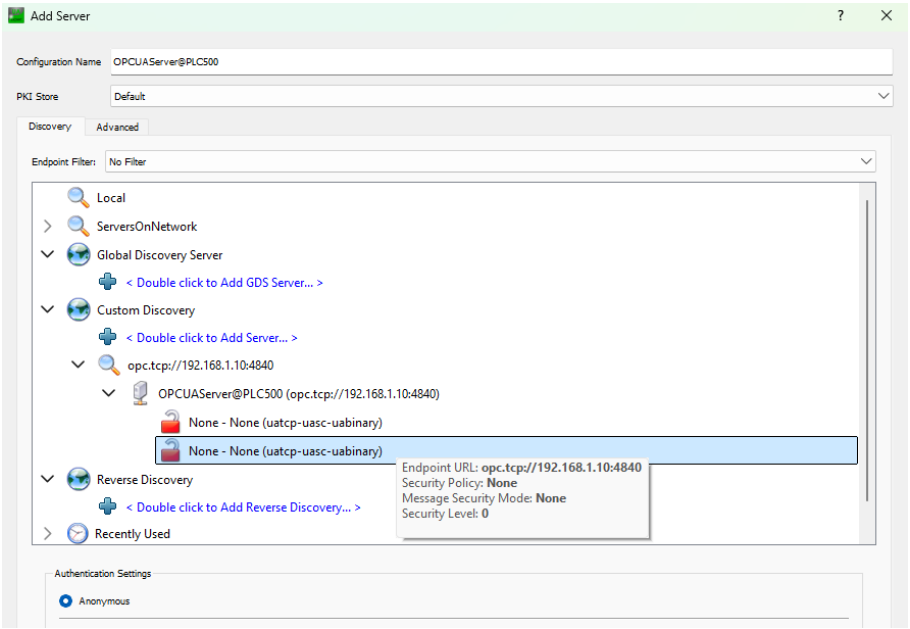


Figura 5.3: *Seleccionando la comunicación sin cifrado.*

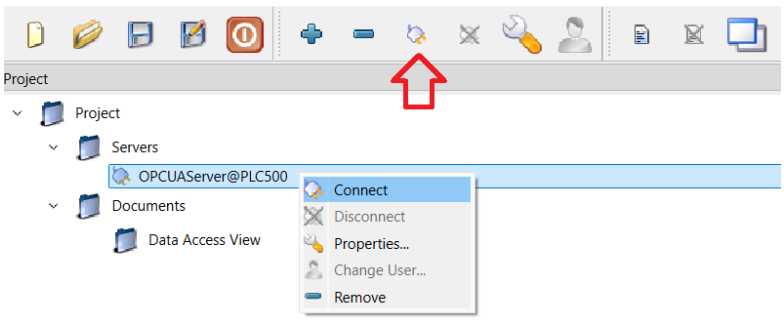


Figura 5.4: *Estableciendo conexión con el Servidor PLC500 OPC UA en UAExpert.*

La conexión se establecerá, y las variables accesibles estarán presentes en **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**. Estas variables pueden seleccionarse y arrastrarse a la ventana **Data Access View**, donde podrán ser monitoreadas en tiempo real, como se muestra en la Figura 5.5 en la pagina 5-3.

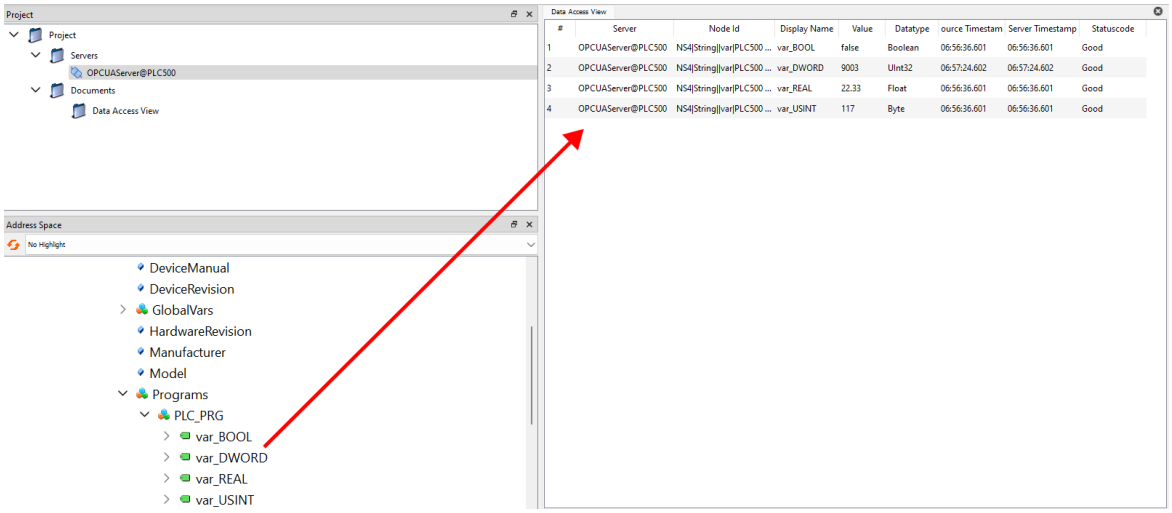


Figura 5.5: *Monitoreo de las variables en UAExpert.*

5.3 CONEXIÓN SEGURA

Para establecer una conexión segura OPC UA con el Servidor del PLC500, es necesario configurar previamente un usuario y un certificado en el PLC. Para más detalles, consulte la Sección 3 CONFIGURACIONES DE SEGURIDAD en la pagina 3-1.

Seleccione una opción de seguridad con credenciales (**Sign**) o con credenciales y cifrado (**SignAndEncrypt**). Haga clic en el ícono correspondiente para habilitar la autenticación, ingrese el usuario configurado en el PLC500, como se muestra en la Figura 5.6 en la pagina 5-3, y haga clic en **OK**.

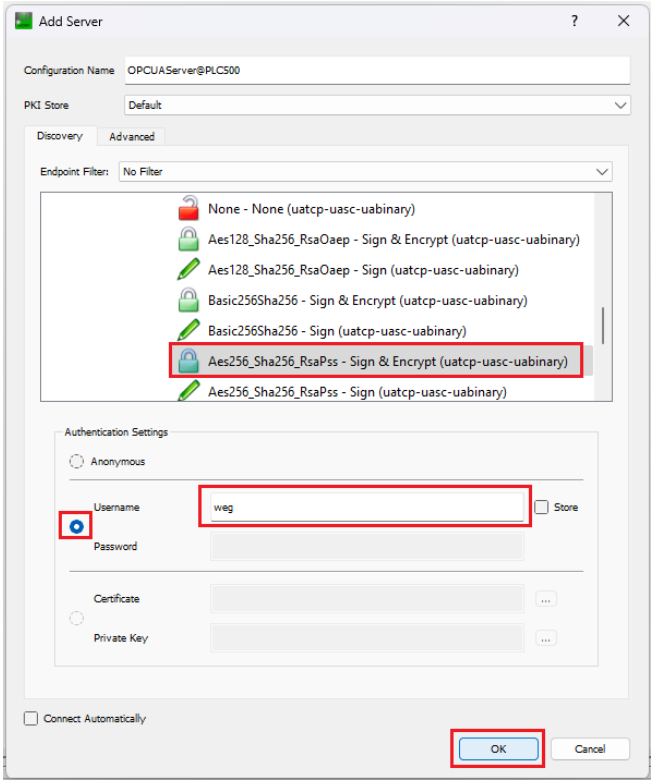
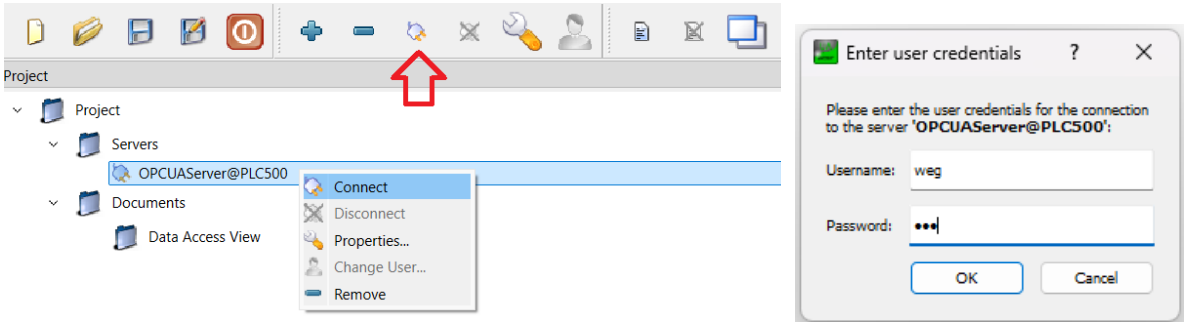


Figura 5.6: *Seleccionando una conexión OPC UA segura en UAExpert.*

El Servidor OPC UA aparecerá debajo de la carpeta **Servers**. Haga clic con el botón derecho sobre él y seleccione **Connect**, o utilice el ícono correspondiente en la barra de herramientas. En la ventana que se abrirá, ingrese la contraseña del usuario configurado y confirme.



¡NOTA!

La advertencia **BadCertificateHostNameInvalid** ocurre cuando el nombre del host en el certificado del Servidor OPC UA no corresponde a la dirección utilizada para la conexión, como al usar una IP en lugar de un nombre de dominio. Si el certificado es confiable y el usuario conoce su origen, la advertencia puede ser ignorada.

Después de hacer clic en **OK**, se mostrará una ventana para confiar en el certificado del PLC500. Haga clic en **Trust Server Certificate** y luego haga clic en **Continue** para finalizar el proceso de confianza y establecer la conexión segura. La Figura 5.7 en la pagina 5-4 muestra las pantallas de validación de certificado de UAExpert.

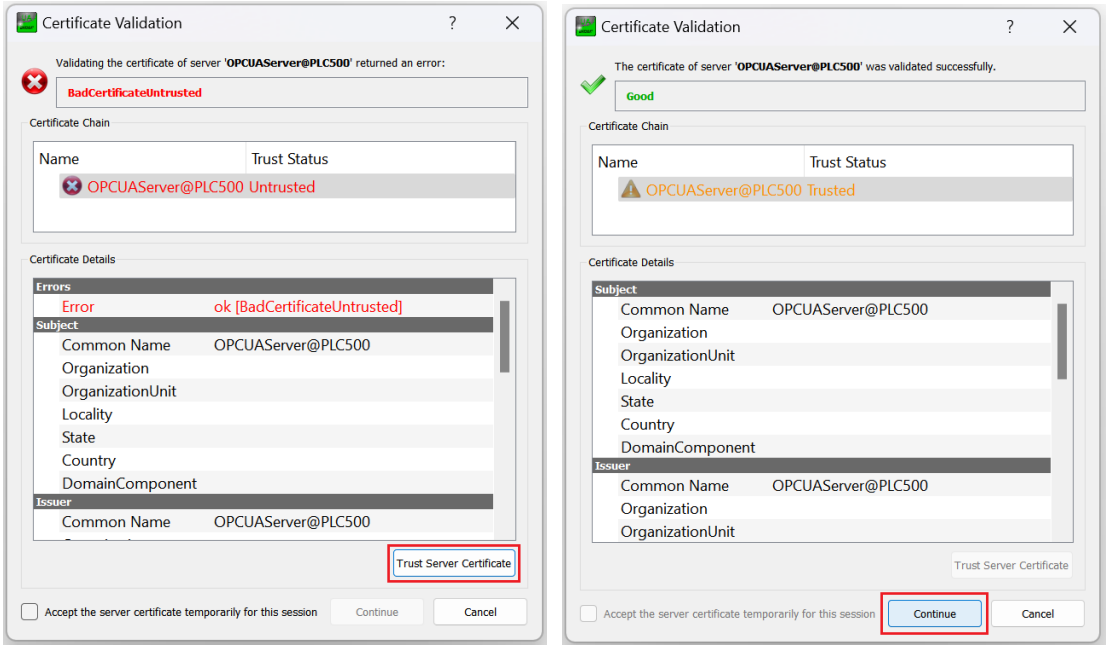
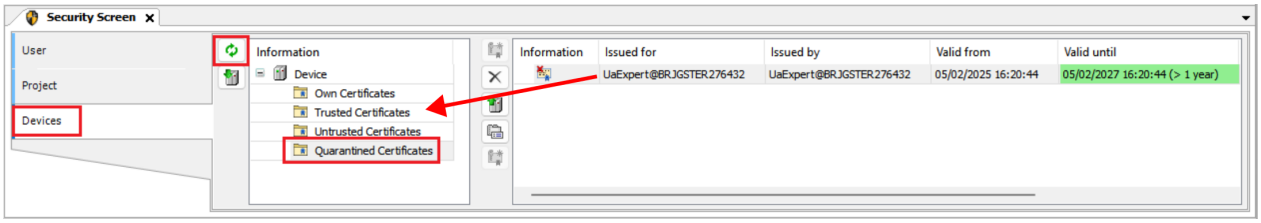
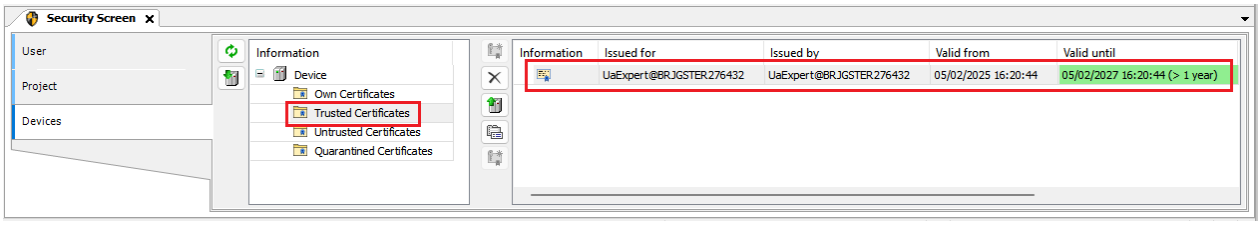


Figura 5.7: *Validación del certificado por UAExpert.*

En CODESYS, vaya a la **Security Screen** y verifique si el certificado del Cliente OPC UA de UAExpert está en cuarentena. Arrástrelo a la carpeta **Trusted Certificates** para agregarlo a la lista de certificados confiables.



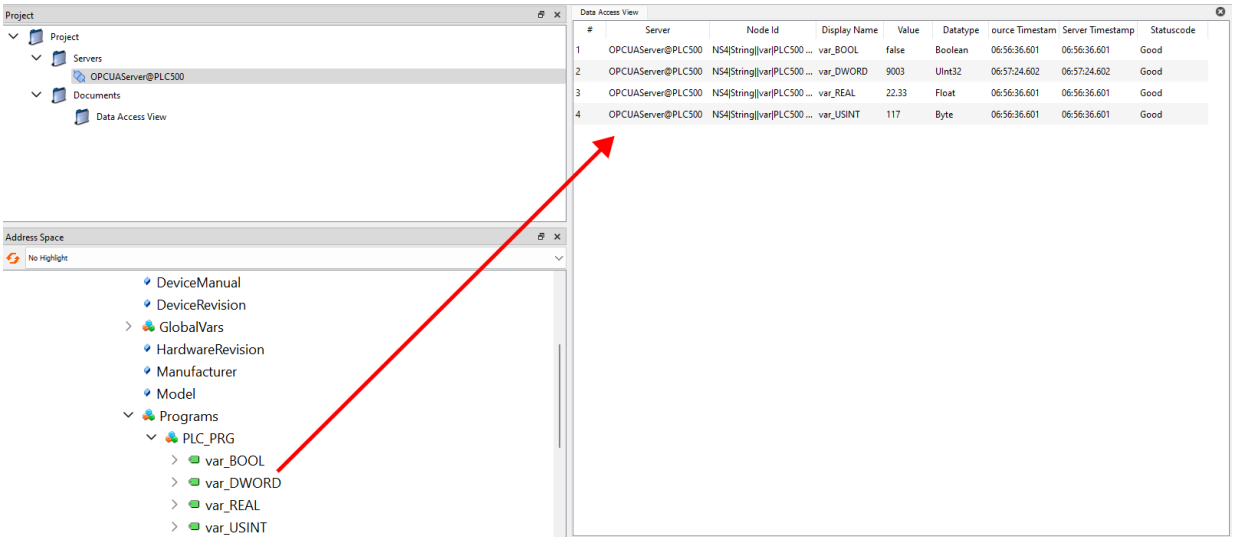
El certificado de UAExpert debe aparecer ahora en la ventana de certificados confiables.



¡NOTA!

Todos los certificados creados y confiables del PLC500 también pueden visualizarse a través del comando **cert-getcertlist** en PLC Shell.

Después de reconectar el Servidor OPC UA en UAExpert, la conexión debe establecerse correctamente. Las variables ubicadas en **Tags** → **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs** pueden arrastrarse a la ventana **Data Access View**, permitiendo que las variables se lean o modifiquen según sea necesario.



¡NOTA!

Cuando un certificado se confía permanentemente, puede utilizarse para establecer otras conexiones seguras en UAExpert hasta que su fecha de validez expire.

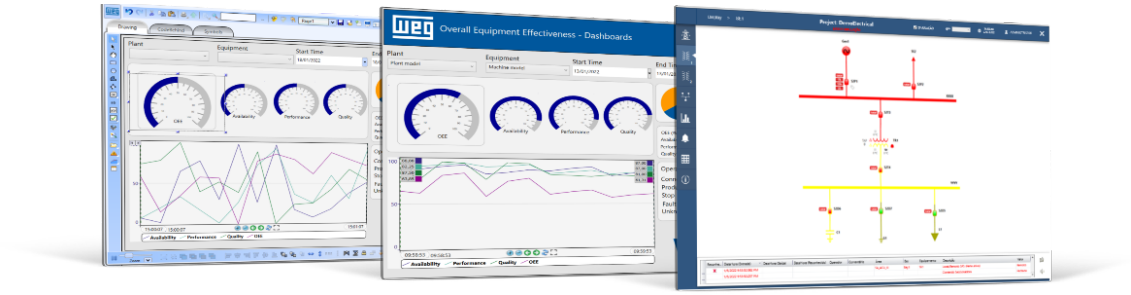
6 CLIENTE OPC UA - WES

Esta sección presenta un ejemplo de configuración de un Cliente OPC UA en **WES (WEGnology Edge Suite)**. Para acceder a la página de WES, visite el sitio web de WEG.

6.1 SOBRE EL WES

La plataforma WEGnology Edge Suite es un software supervisorio moderno y avanzado para control y automatización de procesos industriales y desarrollo de aplicaciones IoT en el borde.

WES es una solución completa, segura, flexible y escalable desde aplicaciones HMI hasta sistemas SCADA avanzados, centros de control y supervisión de procesos industriales distribuidos de misión crítica y alta disponibilidad, incluyendo la versión WES-ELECTRICAL para sistemas eléctricos, permitiendo aplicaciones en los más diversos segmentos de la industria, incluyendo fabricantes de máquinas y equipos (OEMs).



6.2 CREACIÓN DEL PROYECTO

En WES, cree un nuevo proyecto en **Projects** → **New Project**. También es posible verificar la licencia actual de WES en **License**. La Figura 6.1 en la pagina 6-1 presenta la pantalla inicial de WES.

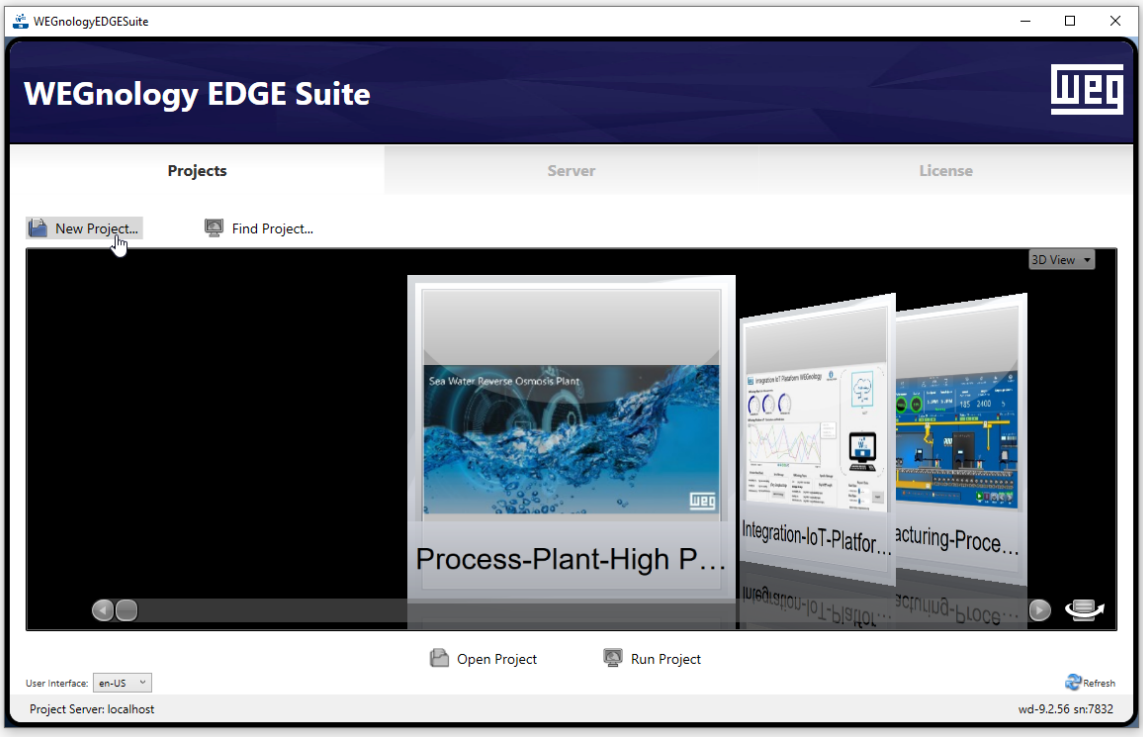


Figura 6.1: *Pantalla inicial de WES.*

Una vez dentro del proyecto creado, se presenta la Figura 6.2 en la pagina 6-2, donde se encuentran los campos principales **Edit**, **Draw** y **Run**.

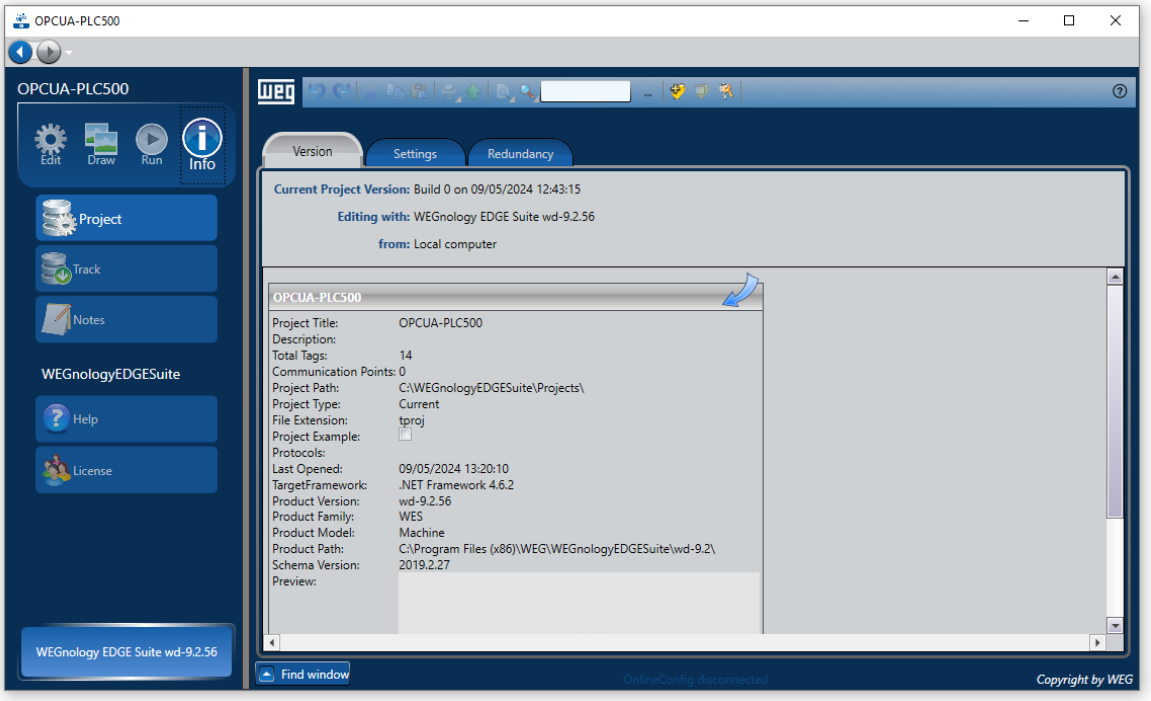


Figura 6.2: *Pantalla inicial del proyecto.*

Vaya a **Edit** → **Devices** → **Channels** y elija **OPCUA - OPC UA Client** en **Installed Protocols**. Luego, haga clic en Channel: **Create new** y **Ok** para crear un nuevo canal. La Figura 6.3 en la pagina 6-2 muestra el canal OPC UA creado.

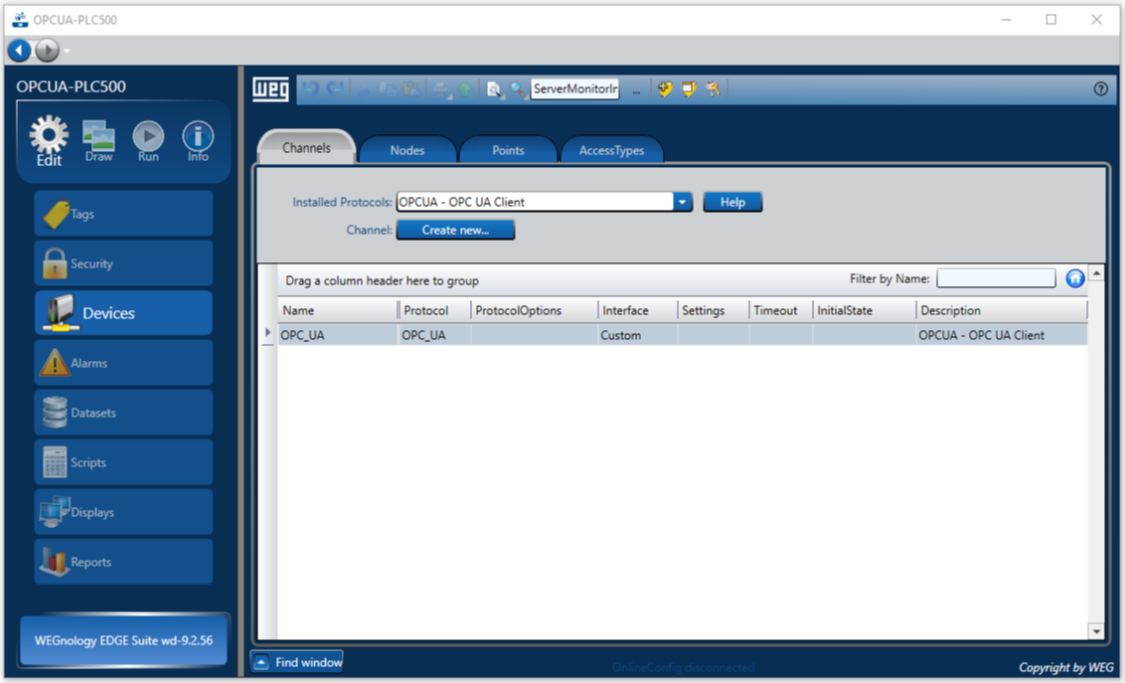


Figura 6.3: *Creando un nuevo canal.*

Para crear un nuevo nodo, vaya a **Edit** → **Devices** → **Nodes** → **New** y haga clic en **Ok**. En la misma ventana, haga clic en el campo en blanco en **PrimaryStation** para abrir la flecha a la derecha. Haga clic en la flecha para abrir el configurador. En **Discovery**, ingrese la dirección IP de la conexión en **IP Address** y haga clic en

Search. Seleccione el dispositivo y luego haga clic en **Ok**. La Figura 6.4 en la pagina 6-3 muestra las pantallas para la creación del nuevo nodo.

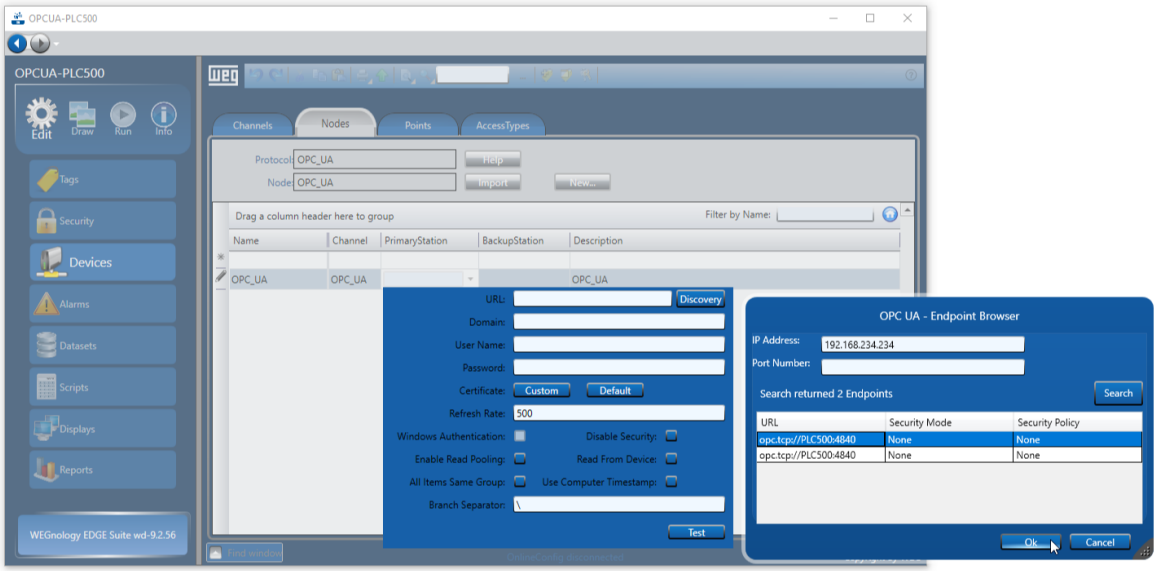


Figura 6.4: *Creando y configurando un nuevo nodo.*

En la URL de la ventana **Discovery**, cambie el nombre del dispositivo a la dirección IP del Servidor OPC UA. Por ejemplo, si la IP es 192.168.1.10, la URL será **opc.tcp://192.168.1.10:4840**. Luego, haga clic en **Test**. Si todo va bien, el mensaje **Connected** se mostrará al lado del botón **Test**. La Figura 6.5 en la pagina 6-3 muestra la prueba para la conexión de un nuevo Servidor OPC UA.

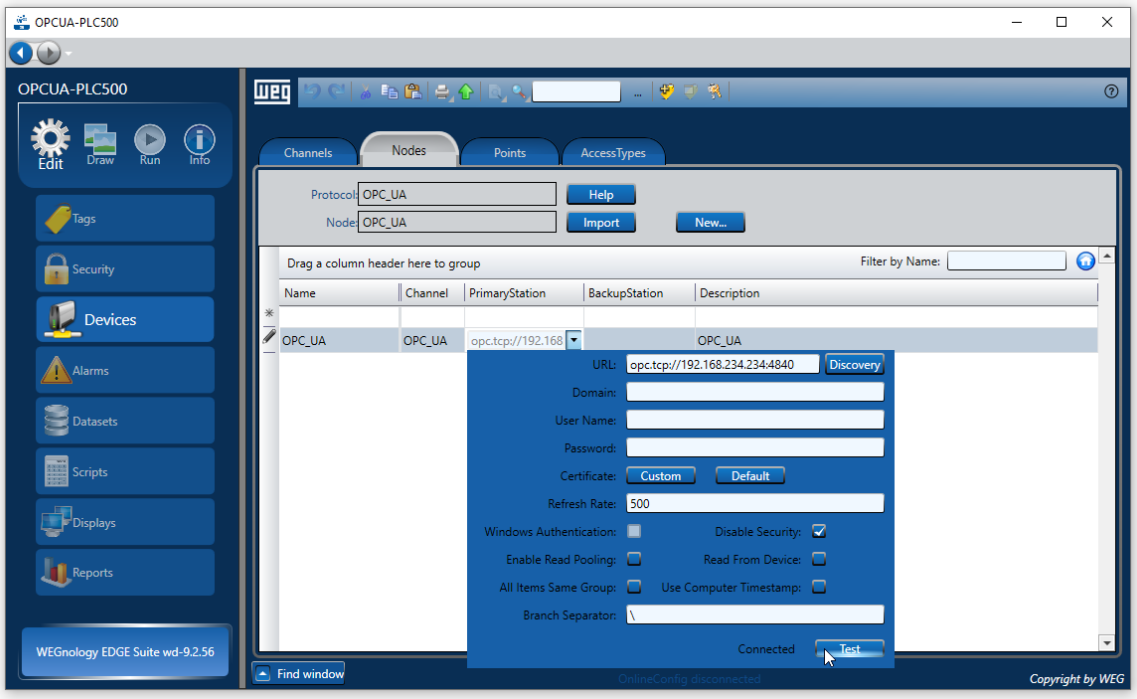


Figura 6.5: *Prueba y conexión de un nuevo Servidor OPC UA.*

Para seleccionar las variables de interés de CODESYS, vaya a **Edit** → **Devices** → **Nodes** → **Import** → **Update**. Puede seleccionar una sola variable, un grupo de variables, POUs o programas enteros. La Figura 6.6 en la pagina 6-4 muestra la importación de variables del Servidor OPC UA.

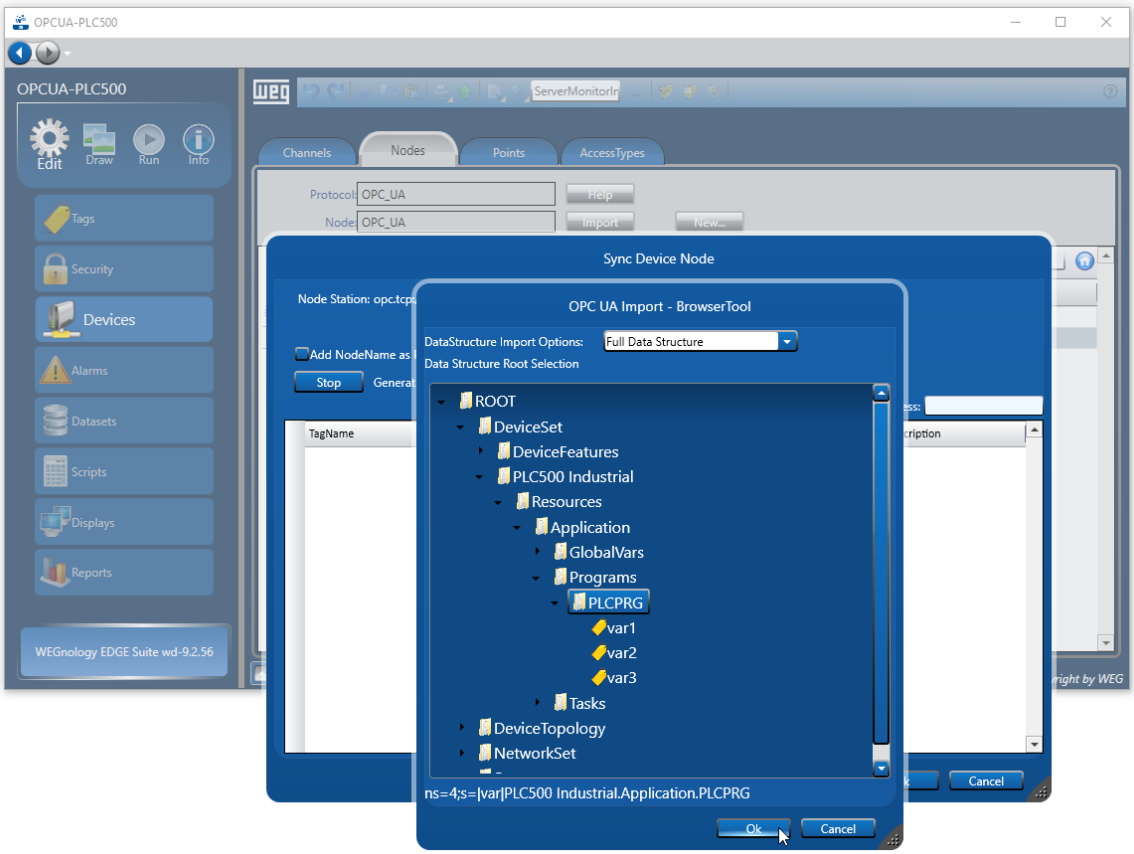


Figura 6.6: *Importando variables del Servidor OPC UA.*

Las variables seleccionadas anteriormente pueden visualizarse en **Edit** → **Devices** → **Points**. Sus permisos pueden modificarse en la opción **AccessType**, cambiando entre **Read**, **Write** o **ReadWrite**. La Figura 6.7 en la pagina 6-4 presenta la pantalla de cambio de permisos de acceso.

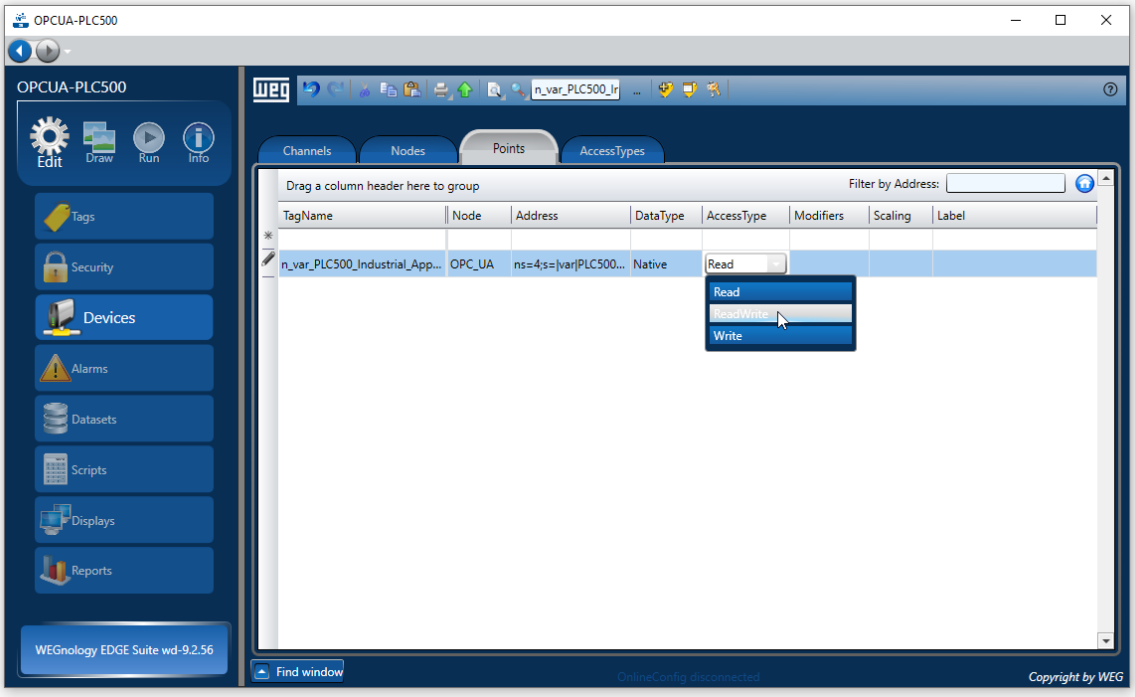


Figura 6.7: *Cambiando permisos de acceso.*

Las variables importadas de CODESYS ahora pueden utilizarse en el sistema SCADA. Por ejemplo, acceda a **Draw** → **Drawing** → **TextBox**. Luego, haga doble clic en el cuadro de texto y vaya a **TextIO** → **ObjectName** → **Tag**, seleccionando la variable apropiada de CODESYS. En la Figura 6.8 en la pagina 6-5 se muestra cómo seleccionar variables de CODESYS para su uso en WES.

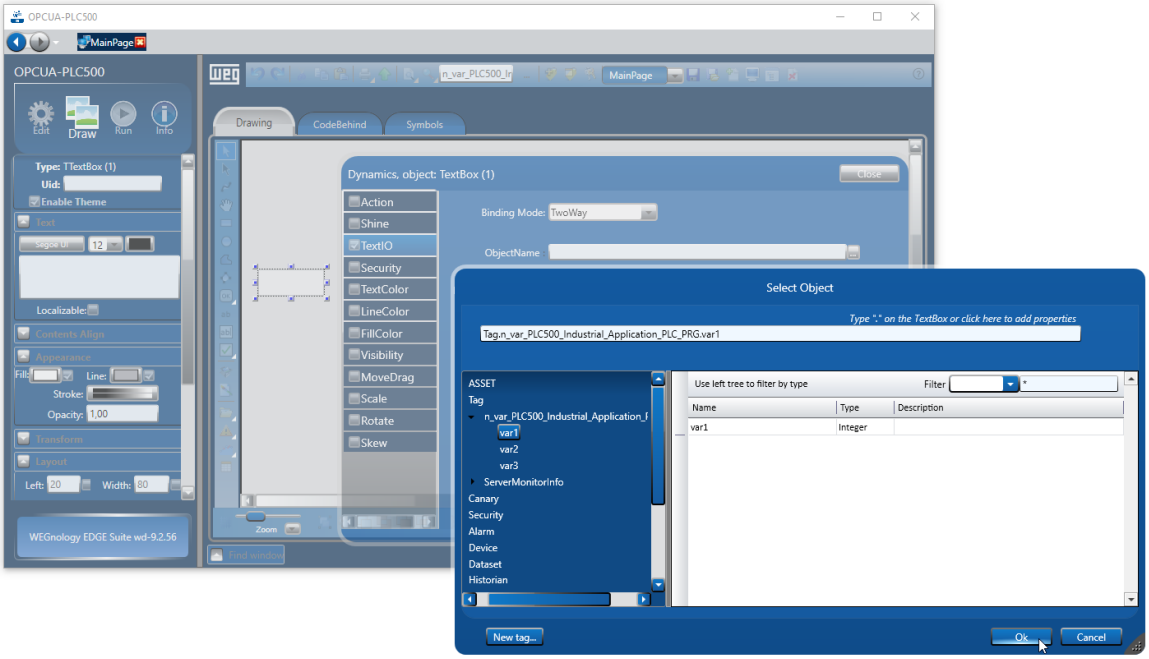


Figura 6.8: *Utilizando las variables de CODESYS en WES vía OPC UA.*

En **Execute** → **Initialization** → **Execute Initialization**, se abre la ventana mostrada en la Figura 6.9 en la pagina 6-5, donde las variables OPC UA de la aplicación pueden ser monitoreadas.

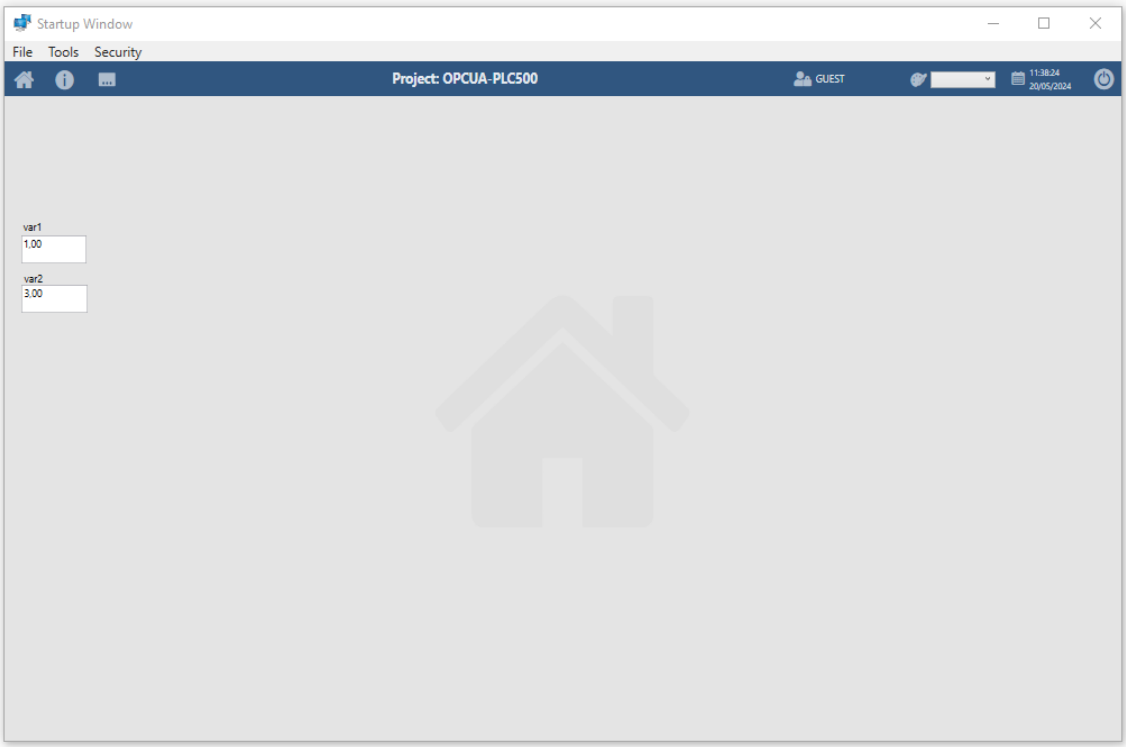


Figura 6.9: *Monitoreo de las variables OPC UA.*

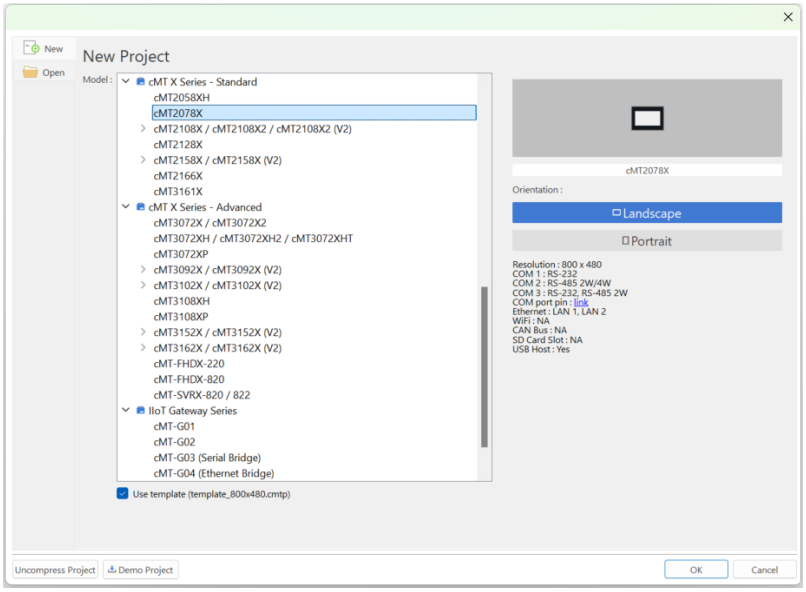
7 CLIENTE OPC UA - EASY BUILDER PRO

Esta sección presenta un ejemplo de configuración de un Cliente OPC UA en Easy Builder PRO utilizando una IHM cMT2078X. El programa puede descargarse en el sitio web de Weintek.

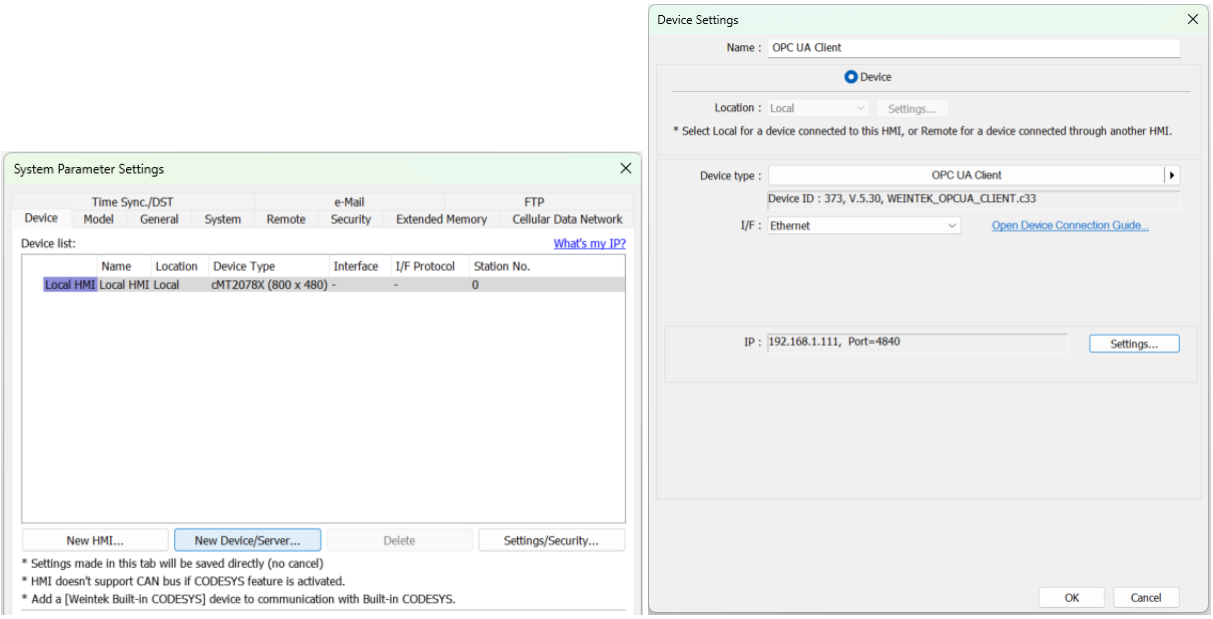
Para comenzar, cree un nuevo proyecto en Easy Builder PRO accediendo a **File** → **New Project**, seleccione el modelo de su IHM y haga clic en **Ok**.

¡NOTA!

Actualmente, los modelos de IHM de WEG que soportan Cliente OPC UA son MT8051iP, MT8072iP, cMT2078X, cMT1106X y cMT2108X2. Para más información, consulte la página del producto en el sitio web de WEG.



A continuación, se abrirá la ventana **System Parameter Settings**. Agregue un nuevo dispositivo en **New Device/Server**. En **Device Type**, seleccione **OPC UA Client**. La interfaz **I/F:** debe estar configurada como **Ethernet** por defecto. Haga clic en **Settings** y defina la dirección IP.



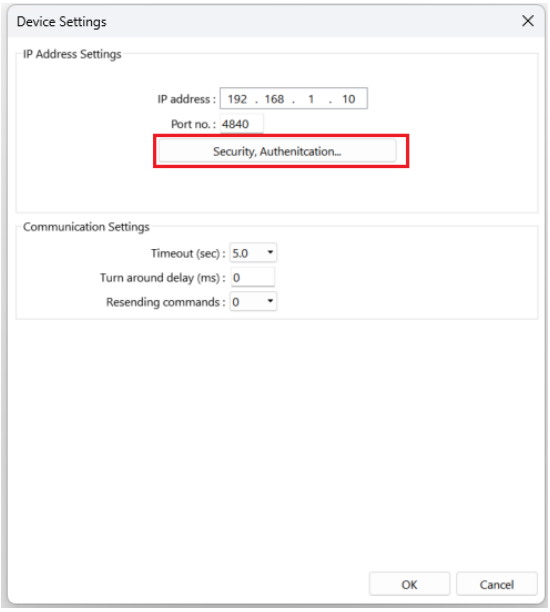
7.1 CONEXIÓN ANÓNIMA

Para que una conexión anónima sea posible, es necesario habilitar en CODESYS la opción **Allow anonymous login** en **Change Runtime Security Policy**. Además, el **CommunicationMode** debe estar configurado como **ALL** para el **CmpOPCUAServer** en **Device Security Settings**. Consulte la Sección 3 CONFIGURACIONES DE SEGURIDAD en la pagina 3-1 para más información.

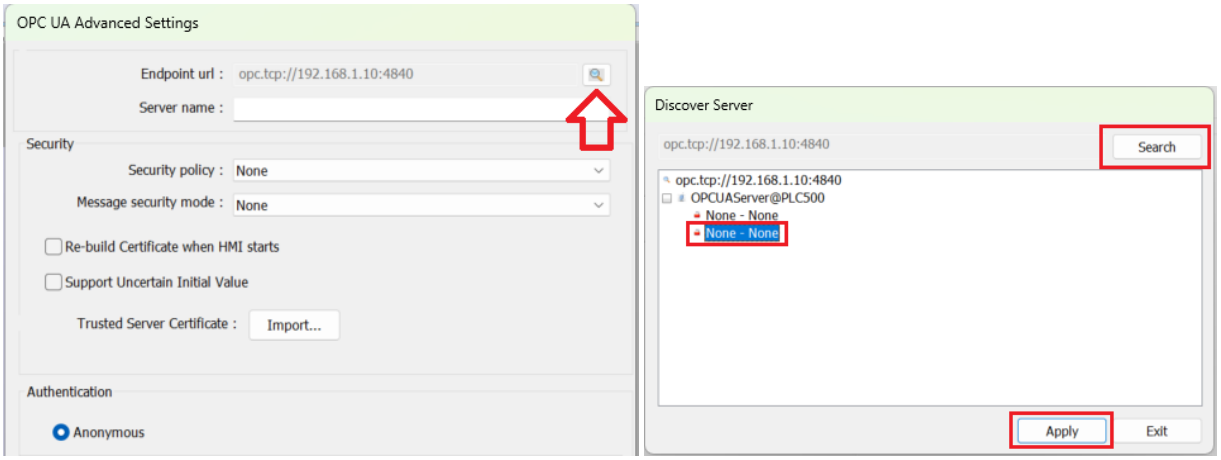
NOTA DE CIBERSEGURIDAD!

El uso de conexión anónima para la operación regular de aplicaciones no se recomienda debido a cuestiones de ciberseguridad. Debe restringirse a fines de prueba, puesta en marcha o cuando no haya otras alternativas disponibles.

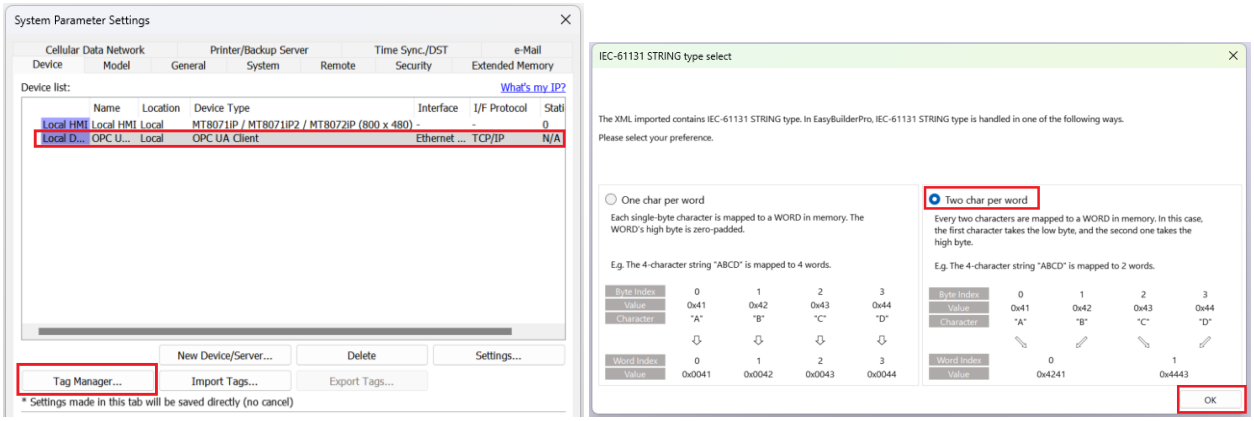
Después de haber configurado la IP del Servidor OPC UA en el PLC500, haga clic en **Security, Authentication**.



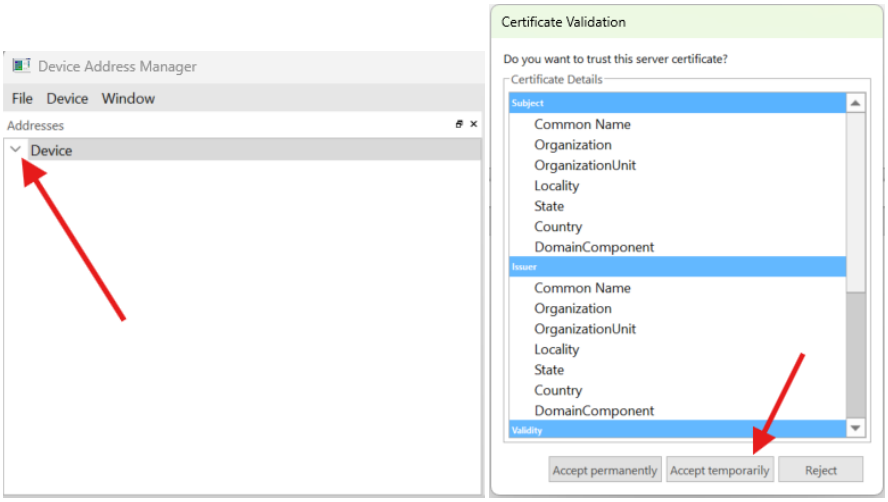
En la ventana **OPC UA Advanced Settings**, haga clic en el ícono . Haga clic en **Search** para detectar los servidores disponibles en la dirección IP configurada. Seleccione una de las opciones de conexión anónima en **None** y haga clic en **Apply**. Mantenga el resto de las configuraciones por defecto y haga clic en **Ok** para cerrar las ventanas hasta volver a **System Parameter Settings**.



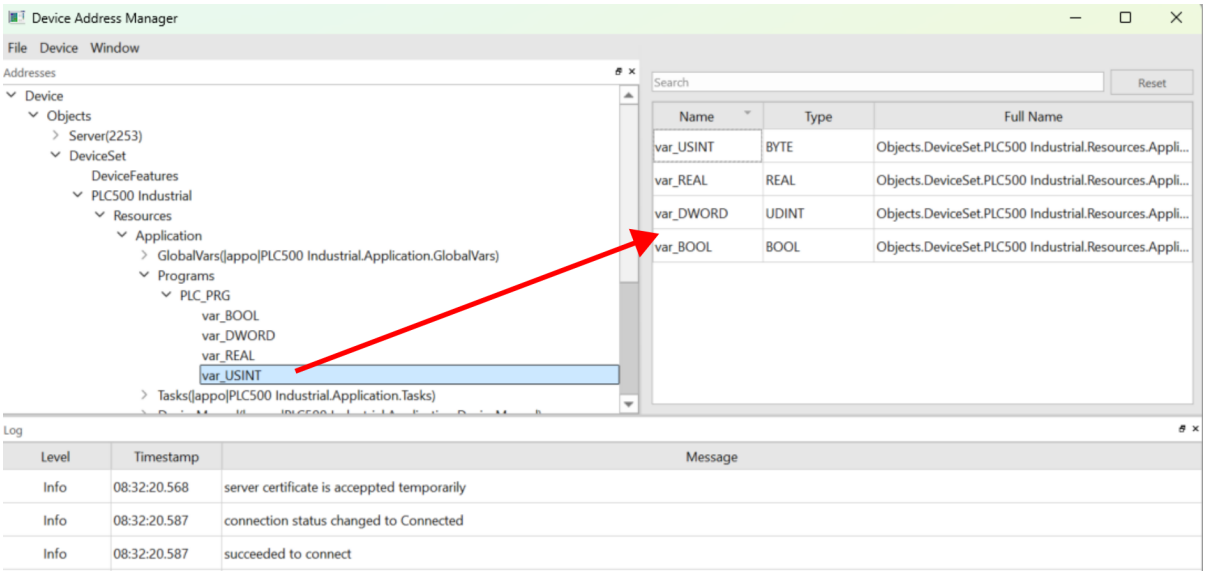
Seleccione el **OPCUA Client** y haga clic en **Tag Manager**. Seleccione una de las opciones de mapeo de las variables y haga clic en **Ok**.



En la ventana **Device Address Manager**, verifique si las opciones **Addresses** y **Log** están habilitadas para visualización en **Window**. Haga clic en la flecha al lado de **Device**. Se abrirá una ventana para aceptar un certificado. Haga clic en **Accept Temporarily**.

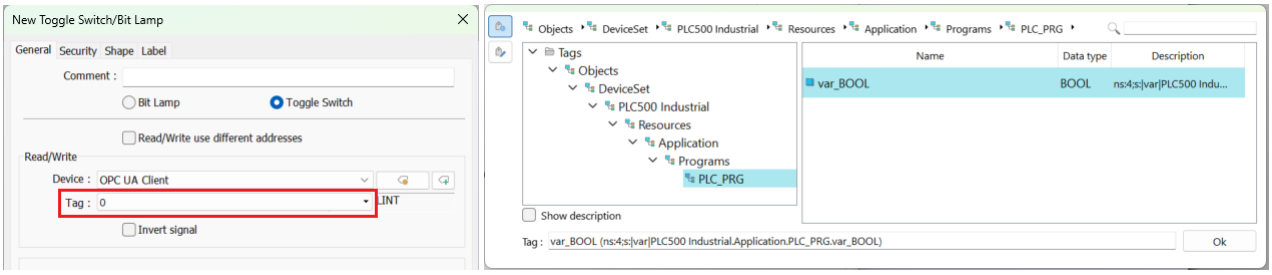


La conexión anónima con el Servidor OPC UA en el PLC500 se establecerá. Haga clic sucesivamente en la flecha en **Object** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**. Todas las variables encontradas en los programas del proyecto CODESYS se mostrarán. En el ejemplo, el proyecto tiene solo un POU llamado **PLC_PRG**. Haga clic en la flecha al lado del programa para ver las variables disponibles para importación en el proyecto de la IHM. Arrastre individualmente cada variable a la ventana al lado.

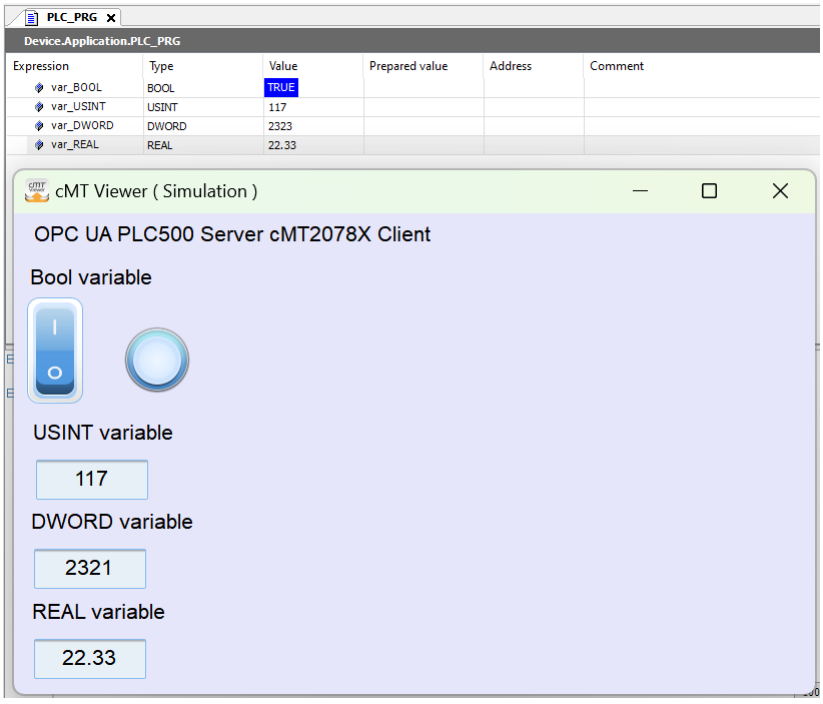


Después de indexar todas las variables de interés del proyecto, vaya a **File** → **Save** y luego **File** → **Exit**. Con las etiquetas importadas, haga clic en **Ok** en la ventana **System Parameter Settings**.

Agregue los objetos deseados en su interfaz y asócielos a las variables del Servidor OPC UA del PLC500 haciendo clic en **Tags**. Haga clic sucesivamente en los íconos **Tags** → **Objects** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**, y seleccione el POU asociado a la variable a ser mapeada.



Después de completar el proyecto de la IHM con todas las variables de interés, compile el proyecto en **Compile** y cargue el programa en la IHM en **Download (PC → HMI)**. La siguiente imagen muestra el monitoreo en línea de las variables en CODESYS y en Easy Builder Pro a través de la **Online Simulation**.



8 CLIENTE OPC UA - PLC500ED

Como se destacó al inicio de este documento, todos los PLCs WEG con CODESYS ofrecen soporte al Servidor OPC UA. Sin embargo, el **PLC500ED** también cuenta con la funcionalidad de **Cliente OPC UA**.

> **¡NOTA!**
>
> El uso del protocolo **Cliente OPC UA** es posible solo en el modelo PLC500ED a través del contenedor **Edge Agent**. No es posible utilizar esta funcionalidad vía CODESYS.

8.1 SOBRE EL PLC500ED

El PLC500ED mantiene todas las funcionalidades del PLC500, pero con la ventaja adicional de soportar procesamiento en el borde (*Edge Computing*) mediante el contenedor **Edge Agent**. Este recurso permite la conexión de equipos industriales a las plataformas en la nube de WEG, como **WEGnology** y **WEG Smart Machine**, posibilitando la implementación de soluciones digitales avanzadas, como monitoreo remoto, mantenimiento predictivo y análisis de datos en tiempo real. Para más detalles sobre el producto o sobre las plataformas, visite el sitio web de WEG.

8.2 CONFIGURACIÓN RÁPIDA

A continuación, se presentan los pasos básicos para configurar rápidamente una aplicación WEGnology a través del PLC500ED.

1. Crear una aplicación en el sitio web WEGnology y guardar sus credenciales o obtener las credenciales de una aplicación WEG Digital Solution.
2. Conectar el PLC500ED a internet mediante la página web o CODESYS.
3. Insertar los datos de la aplicación en la pestaña **Cloud Integration** de la página web.
4. Habilitar el contenedor **Edge Agent** en la pestaña **Docker** de la página web.
5. Verificar si el dispositivo fue reconocido automáticamente como en línea en la plataforma. En este momento, el **PLC500ED** estará listo para realizar el *deploy* de la aplicación Cliente OPC UA o cualquier otro *workflow*.

Con todas las configuraciones realizadas correctamente, la página de estado del PLC500ED debe mostrar que el producto está conectado a internet, con una aplicación también conectada y con el contenedor Edge Agent en funcionamiento, como se muestra en la Figura 8.1 en la pagina 8-2.

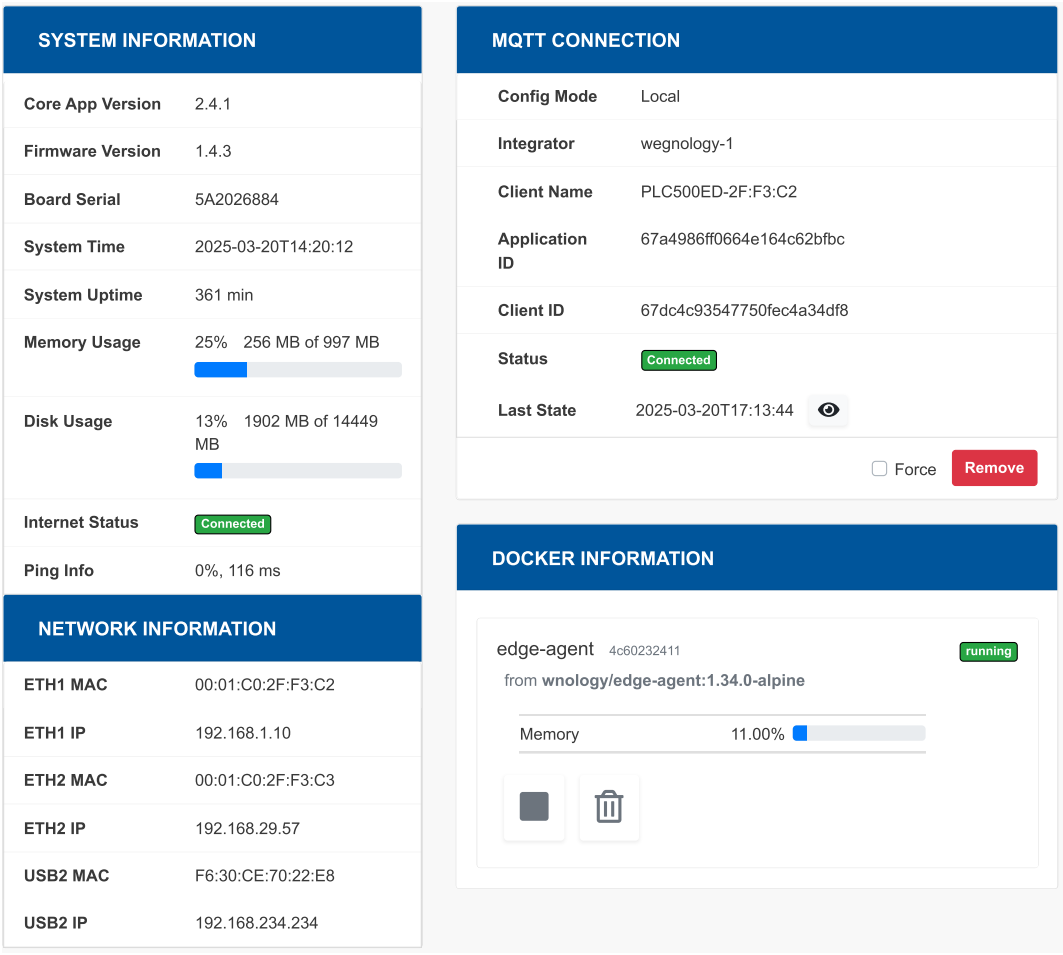


Figura 8.1: *Pantalla de estado del PLC500ED.*

Para más detalles, consulte la Nota de Aplicación del PLC500ED, disponible en el sitio web de WEG.

8.3 OPC UA PING PONG

Este ejemplo básico de aplicación utiliza un **PLC500ED** como **Cliente OPC UA** y un **PLC410** como **Servidor OPC UA**. Cada 5 segundos, el Cliente lee la variable **iVar** del Servidor. Si el valor es 1, el Cliente escribe 0 en **iVar**. Paralelamente, el Servidor, a través de CODESYS, también lee **iVar**. Si el valor es 0, el Servidor escribe 1 en **iVar** e incrementa **iCount**.

¡NOTA!

La interfaz **ETH1** del **PLC500ED** debe estar conectada a la interfaz **ETH** del **PLC410**.

8.3.1 Servidor OPC UA - PLC410

El PLC410 debe estar con la **ETH** configurada con la dirección IP **192.168.1.20** y ejecutando una aplicación Servidor OPC UA en CODESYS, con las variables iVar (INT) e iCount (INT) exportadas.

¡NOTA!

Cualquier PLC de WEG con CODESYS puede utilizarse como **Servidor OPC UA**, siempre que esté previamente configurado, como se detalla en la Sección 4 SERVIDOR OPC UA - CODESYS en la pagina 4-1.

La Figura 8.2 en la pagina 8-3 muestra la declaración de variables y la Figura 8.2 en la pagina 8-3 presenta el programa CODESYS en texto estructurado para la aplicación OPCUA_PingPong.

OPCUA_PingPong

```
PROGRAM OPCUA_PingPong
VAR

  iVar : INT := 0;
  iCount : INT := 0;

END_VAR
```

Figura 8.2: Declaración de variables OPCUA_PingPong.

OPCUA_PingPong - Structured Text (ST)

```
IF iVar = 0 THEN iVar := 1; iCount := iCount + 1; END_IF
IF iCount > 1000 THEN iCount := 0; END_IF
```

Figura 8.3: Programa OPCUA_PingPong en texto estructurado.

8.3.2 Cliente OPC UA - PLC500ED

El PLC500ED debe estar con la **ETH1** configurada con la dirección IP **192.168.1.10**, conectado a internet a través de la **ETH2**, ejecutando el contenedor **Edge Agent** y con una aplicación WEGnology debidamente configurada. No se necesita ninguna aplicación de CODESYS.

En la página principal de la plataforma WEGnology, vaya a **Workflows** → **Edge Workflows** → **Add**. Cree el *workflow* mostrado en la Figura 8.4 en la pagina 8-3, compuesto por los bloques **Timer**, **OPC UA: Read**, **Conditional** y **OPC UA: Write**.

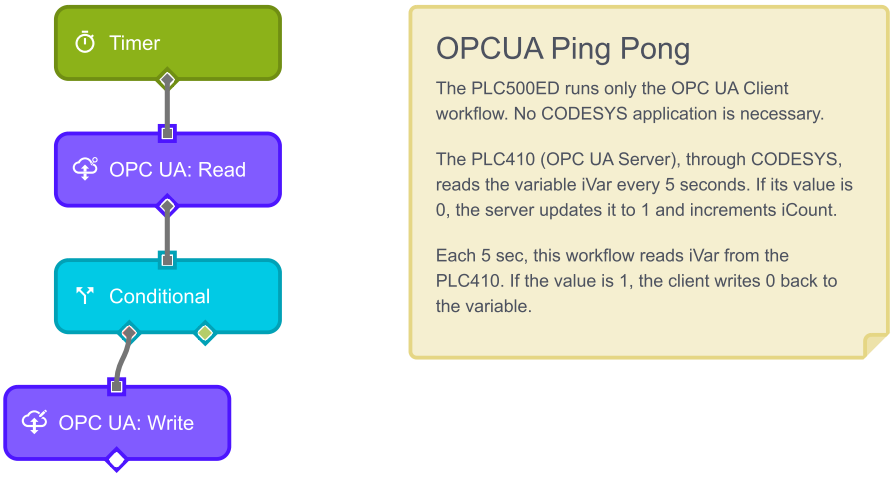


Figura 8.4: Workflow Cliente OPC UA.

A continuación se describen los bloques y las configuraciones utilizadas:

Timer: define la periodicidad de la ejecución del flujo. Utilizado: 5 segundos.
OPC UA: Read: realiza la lectura de variables en el Servidor OPC UA. Se utilizan las siguientes configuraciones:

- OPC UA URI Template: opc.tcp://192.168.1.20:4840
- Namespace: 4
- Identifier Template: s=|var|PLC410 Industrial.Application.OPCUA_PingPong.iVar
- Result Key: iVar
- Destination Path: {data}

Conditional: evalúa una condición lógica basada en los valores leídos. Condición utilizada: `{{iVar}} === '1'`.
OPC UA: Write: ejecuta la escritura de variables en el Servidor OPC UA. Se utilizan las siguientes configuraciones:

- OPC UA URI Template: opc.tcp://192.168.1.20:4840
- Namespace: 4
- Identifier Template: s=|var|PLC410 Industrial.Application.OPCUA_PingPong.iVar
- Value Source Type: 0

¡NOTA!

Si es necesario confirmar el **Namespace Index** o el **Identifier** de las variables, puede ser útil utilizar **UAExpert**. En **UAExpert**, al acceder al Servidor OPC UA, es posible visualizar el **NodeID**, que muestra estas variables en el formato: ns=4;s=|var|PLC410 Industrial.Application.OPCUA_PingPong.

Al finalizar el *workflow*, vaya a la esquina superior derecha de la pantalla, haga clic en **Deploy**, seleccione el dispositivo e instale la aplicación en **Deploy Version**.

BRASIL
WEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.
Av. Prefeito Waldemar Grubba, 3000
89256-900 - Jaraguá do Sul - SC
Teléfono: 55 (47) 3276-4000
Fax: 55 (47) 3276-4060
www.weg.net