

# OPC UA<sup>®</sup> PLC500, PLC500ED, PLC500MC PLC410

Nota de Aplicação





# Nota de Aplicação

# PLC410, PLC500, PLC500ED, PLC500MC

Documento: 10013132240

Revisão: 00

Data de publicação: 04/2025

A informação abaixo descreve as revisões ocorridas neste manual.

Versão	Revisão	Descrição
1.4.2	R00	Primeira edição.

1	IN7 1.1 1.2 1.3 1.4 1.5	<b>TRODUÇÃO</b> ABREVIAÇÕES E DEFINIÇÕES UTILIZADAS O PROTOCOLO OPC UA DOCUMENTOS DE REFERÊNCIA AVISO IMPORTANTE SOBRE SEGURANÇA CIBERNÉTICA E COMUNICAÇÕES MARCAS REGISTRADAS	<b>1-1</b> 1-2 1-2 1-2 1-2 1-2
2			2-1
	2.1		2-1
	2.3	TOPOLOGIAS DE REDE OPC UA	2-2
3	СС	NFIGURAÇÕES DE SEGURANÇA	3-1
	3.1	CODESYS SECURITY AGENT	3-1
	3.2	RUNTIME CODESYS	3-1
	3.3 3.4	CONFIGURAÇÕES DE SEGURANÇA DO OPC UA CRIAÇÃO DE CERTIFICADO AUTOASSINADO	3-3 3-4
4	SE	RVIDOR OPC UA - CODESYS	4-1
5	CL	IENTE OPC UA - UA EXPERT	5-1
	5.1	ENCONTRANDO SERVIDORES PELO URL	5-1
	5.2	CONEXÃO ANÔNIMA	5-2
	5.3	CONEXÃO SEGURA	5-3
6	CL	IENTE OPC UA - WES	6-1
	6.1	SOBRE O WES	6-1
	6.2	CRIAÇAO DO PROJETO	6-1
7	CL	IENTE OPC UA - EASY BUILDER PRO	7-1
	7.1		7 <b>-2</b>
8	CL	IENTE OPC UA - PLC500ED	8-1
	8.1	SOBRE O PLC500ED	8-1
	8.2		8-1
	8.3	0 PC UA PING PUNG	8-2 0 0
		0.3.1 Servicior OPC UA - PLC410	0-2
		0.3.2 Gliente OFG UA - FLGOUVED	0-3

# 1 INTRODUÇÃO

Esta Nota de Aplicação destina-se a auxiliar no uso do protocolo **OPC UA**<sup>®</sup> nos PLCs da WEG, modelos PLC410, PLC500, PLC500ED e PLC500MC. Ao longo deste documento, o PLC500 é utilizado como exemplo, porém as informações apresentadas são igualmente aplicáveis aos demais modelos mencionados. Salienta-se que os dados fornecidos podem mudar ligeiramente por conta do contínuo desenvolvimento e atualização dos produtos e das ferramentas.

Além de fornecer um panorama geral sobre o uso do protocolo OPC UA, este documento apresenta as interfaces de comunicação, recomendações de instalação, configurações de segurança, exemplos de topologias de rede e um guia para estabelecer a comunicação OPC UA entre os PLCs e diferentes dispositivos e softwares, atuando tanto como Servidor quanto como Cliente. Vale destacar que todos os PLCs WEG com **CODESYS**<sup>®</sup> incluem suporte para o Servidor OPC UA. A funcionalidade de Cliente OPC UA é disponibilizada exclusivamente pelo PLC500ED, por meio da programação na plataforma WEGnology.

Para mais informações a respeito do hardware, interfaces e protocolos de comunicação, consulte o Manual do Usuário do respectivo produto, disponível no site da WEG. Para uma descrição mais profunda e detalhada sobre OPC UA, acesse a ajuda online em CODESYS Online Help.



#### ATENÇÃO!

Esta nota de aplicação é direcionada para profissionais treinados em redes industriais. A instalação e configuração dos dispositivos deve ser feita de acordo com o manual do fabricante.

# NOTA!

Recomenda-se utilizar o **CODESYS** versão **V3.5 SP19** ou superior, bem como a versão mais recente das bibliotecas de configuração para OPC UA.

# 1.1 ABREVIAÇÕES E DEFINIÇÕES UTILIZADAS

**CA**: Entidade pública ou privada que faz parte da cadeia de confiança da certificação digital, responsável por emitir, revogar e renovar certificados digitais (*Certificate Authority*).

**CODESYS**: Plataforma de programação que permite desenvolver, configurar e monitorar soluções para automação industrial e integração de sistemas.

Edge Agent: Container previamente instalado no PLC500ED que permite a execução local de Edge Workflows.

**IoT**: Sigla que refere-se às tecnologias que facilitam a comunicação e a troca de dados entre dispositivos e a nuvem, bem como entre os próprios dispositivos (*Internet of Things*).

**IIoT**: Aplicação de tecnologias IoT no contexto industrial, conectando dispositivos, máquinas e sistemas via Internet para coleta, troca e análise de dados, visando maior eficiência, automação e monitoramento (*Industrial Internet of Things*).

**OPC UA**: Protocolo de comunicação industrial que garante interoperabilidade segura entre dispositivos e sistemas. Ele oferece criptografia, autenticação e suporte a modelos de dados complexos, sendo amplamente usado em automação e IIoT (*Open Platform Communications Unified Architecture*).

**SCADA**: Sistema que monitora e controla processos industriais em tempo real, coletando dados de sensores e dispositivos locais e remotos para análise e operação centralizada (*Supervisory Control and Data Acquisition*).

**UAExpert**: Software utilizado como um Cliente OPC UA de teste de uso geral, suportando recursos como *DataAccess, Alarms & Conditions,* Acesso Histórico e chamada de Métodos UA.

**WEGnology**: Plataforma IIoT da WEG para monitoramento, análise e automação de processos industriais, permitindo a conexão de dispositivos e a gestão de dados em tempo real.

**WES**: WEGnology Edge Suite é um moderno e avançado software para supervisão, controle e automação de processos industriais e desenvolvimento de aplicações Edge IoT.

# 1.2 O PROTOCOLO OPC UA

O OPC UA (*Open Platform Communications Unified Architecture*) é um protocolo de comunicação industrial independente de plataforma que garante interoperabilidade segura e confiável entre dispositivos, máquinas e sistemas de diferentes fabricantes. Desenvolvido e mantido pela **OPC Foundation**, foi projetado para substituir versões anteriores do OPC, oferecendo suporte a modelos de informação complexos e segurança avançada, incluindo criptografia e autenticação.

O padrão OPC é uma série de especificações desenvolvidas por fornecedores da indústria, usuários finais e desenvolvedores de software. Essas especificações definem a interface entre Clientes e Servidores, incluindo acesso a dados em tempo real, monitoramento de alarmes e eventos. Amplamente utilizado em automação industrial, SCADA, IIoT e integração de sistemas, o OPC UA padroniza a troca de dados em diversos ambientes.

No **CODESYS**, o OPC UA está integrado como Servidor nativo, permitindo que Clientes OPC UA acessem variáveis do dispositivo de forma estruturada e segura. A configuração ocorre no **Symbol Configuration**, onde os dados compartilhados podem ter controle de acesso de leitura e escrita. Com suporte a criptografia e autenticação, esse protocolo facilita a comunicação entre CLPs e sistemas industriais. Para mais detalhes, consulte a documentação oficial no site do CODESYS e do OPC Foundation.

# 1.3 DOCUMENTOS DE REFERÊNCIA

Recomenda-se a consulta dos documentos relacionados ao OPC UA mostrados na Tabela 1.1 na página 1-2.

Tabela 1.1: Documentos de referência.

Documento	Versão	Fonte
Practical Security Recommendations for building OPC UA Applications	3	OPC Foudation

# 1.4 AVISO IMPORTANTE SOBRE SEGURANÇA CIBERNÉTICA E COMUNICAÇÕES

Os CLPs da WEG, modelos PLC410, PLC500, PLC500ED e PLC500MC, possuem a capacidade de se conectar e trocar informações por meio de redes e protocolos de comunicação. Embora tenham sido projetados e testados para garantir o funcionamento adequado com outros sistemas de automação utilizando os protocolos mencionados neste manual, é essencial que o cliente compreenda as responsabilidades associadas à informação e à cibersegurança ao utilizar este equipamento.

Portanto, é de inteira responsabilidade do cliente adotar estratégias de defesa em profundidade e implementar políticas e medidas para garantir a segurança do sistema como um todo, incluindo as comunicações enviadas e recebidas pelo equipamento. Essas medidas incluem, mas não se limitam a, instalação de firewalls, programas antivírus e antimalware, criptografia de dados, controle de autenticação e controle físico de acesso dos usuários.

A WEG e suas afiliadas não se responsabilizam por danos ou perdas decorrentes de violações de segurança cibernética, incluindo, mas não se limitando a, acesso não autorizado, intrusão, vazamento e/ou roubo de dados ou informações, negação de serviço ou qualquer outra forma de violação de segurança. A utilização deste produto em condições para as quais não foi especificamente projetado não é recomendado e pode acarretar danos ao produto, à rede e ao sistema de automação.

Neste sentido, é imprescindível que o cliente compreenda que intervenções externas por meio de programas de terceiros, a exemplo dos sniffers ou programas com ações semelhantes, possuem o potencial de ocasionar interrupções ou restrições na funcionalidade do equipamento.

#### 1.5 MARCAS REGISTRADAS

OPC UA<sup>®</sup> é marca registrada da OPC Foundation.

Todas as outras marcas registradas são propriedades de seus respectivos titulares.

# 2 INTERFACE ETHERNET

A comunicação OPC UA é realizada através das conexões Ethernet, indicadas na Figura 2.1 na página 2-1 para o PLC500 e PLC410. Inicialmente, cada porta Ethernet possui o endereço de IP indicado na Tabela 2.1 na página 2-1, podendo ser alterado a qualquer momento através do software CODESYS.



Figura 2.1: Indicação das conexões Ethernet dos PLCs. (a) PLC500 e (b) PLC410.

Tabela 2.1: Endereços padrão para as portas Ethernet.

PLC410	PLC500	Endereço de IP padrão
ETH	ETH1	192.168.1.10
-	ETH2	192.168.2.10

A distribuição dos pinos do conector segue o padrão Ethernet 1000BASE-TX. A interface Ethernet do PLC410 suporta velocidades de até 100 Mbps, enquanto as interfaces Ethernet do PLC500 alcançam até 1000 Mbps.

Os PLCs PLC500, PLC500ED e PLC500MC possuem duas interfaces Ethernet, que podem ser configuradas no modo **Independent**, no qual as interfaces operam com IPs distintos, ou no modo **Switch**, onde as interfaces compartilham o mesmo endereço IP.

As interfaces Ethernet são compatíveis com diversos protocolos de comunicação, incluindo o OPC UA, e podem ser utilizadas simultaneamente para múltiplos protocolos. Para instruções sobre como configurar essas redes adicionais, consulte as Notas de Aplicação do produto disponíveis no site da WEG.

# 2.1 LEDS DE INDICAÇÃO

As portas Ethernet possuem LEDs para indicação de velocidade e link/atividade da rede, como indicado na Figura 2.2 na página 2-2. Estes LEDs possuem o comportamento descrito pela Tabela 2.2 na página 2-2 e Tabela 2.3 na página 2-2.



Figura 2.2: Leds de velocidade (S1) e link/atividade (L1) da interface Ethernet do PLC500.

Tabela 2.2: LED S1 - Velocidade.

Estado	Descrição
Apagado	Equipamento desligado ou link de 10 Mbps
Verde, sólido	Link de 100 Mbps

Tabela 2.3: LED L1 - Link/Atividade.

Estado	Descrição
Apagado	Equipamento desligado ou sem link
Âmbar, sólido	Com link e sem atividade na rede
Âmbar, piscando	Com link e com atividade na rede

# 2.2 INSTALAÇÃO DA REDE OPC UA

A rede OPC UA, como várias redes de comunicação industriais, pelo fato de ser aplicada muitas vezes em ambientes agressivos e com alta exposição à interferência eletromagnética, exige certos cuidados que devem ser tomados para garantir uma baixa taxa de erros de comunicação durante a sua operação.



#### ATENÇÃO!

Recomenda-se a utilização de componentes passivos (cabos, conectores, switchs, hubs) certificados para aplicações industriais.

As características recomendadas para o cabo utilizado na instalação são:

- Cabo padrão Ethernet, 1000Base-TX, CAT 5e ou superior.
- Cabo blindado.
- Comprimento máximo de 100 m para conexão entre equipamentos.

Uma conexão adequada ao sistema de aterramento é essencial para minimizar problemas de interferência eletromagnética em ambientes industriais. É importante evitar a conexão do cabo em múltiplos pontos de aterramento, especialmente em locais onde há diferenças de potencial entre os pontos de terra. Além disso, recomenda-se que os cabos de sinal e comunicação sejam instalados em rotas dedicadas, mantendo distância dos cabos de potência.



#### PERIGO!

Instalações de aterramento inadequadas podem causar falhas na rede OPC UA e representar risco de choque elétrico fatal.

# 2.3 TOPOLOGIAS DE REDE OPC UA

As topologias de rede em um sistema OPC UA podem variar conforme as necessidades do projeto e a arquitetura da instalação. Na Figura 2.3 na página 2-3 tem-se um exemplo de topologia em estrela, na qual um switch central conecta todos os dispositivos clientes e servidores OPC UA.



Figura 2.3: Exemplo de topologia de rede OPC UA integrada a outros protocolos de comunicação utilizados em ambientes industriais.

Na figura, a IHM pode atuar como Servidor OPC UA para um sistema SCADA, como o WES rodando em um computador, ao mesmo tempo em que se comporta como Cliente dos PLCs PLC500 e PLC410. Além disso, é possível estabelecer comunicação direta entre os PLCs, onde um pode ser configurado como Servidor e o outro como Cliente OPC UA, permitindo a troca de dados de forma estruturada.

Para controle e monitoração de dispositivos industriais, tanto o PLC500 quanto o PLC410 suportam diversos protocolos de comunicação, incluindo CANopen, Modbus RTU, Modbus TCP, EtherNet/IP, PROFINET e EtherCAT, garantindo integração com uma ampla gama de equipamentos e redes industriais. Essa flexibilidade possibilita desde a comunicação com sensores e atuadores até a interligação com sistemas avançados de supervisão e controle distribuído.



# NOTA!

Para mais informações sobre os protocolos de comunicação do PLC500 e PLC410, consulte as Notas de Aplicação disponíveis nas suas respectivas páginas de produto no site da WEG.

# 3 CONFIGURAÇÕES DE SEGURANÇA

Nesta seção, são detalhadas as opções de segurança para a comunicação OPC UA do PLC500 no CODESYS. As configurações podem ser ajustadas conforme os requisitos de cada aplicação, no entanto, recomenda-se sempre utilizar o mais alto nível de segurança disponível.

# 3.1 CODESYS SECURITY AGENT

O complemento **CODESYS Security Agent** permite configurar e gerenciar aspectos essenciais de segurança no ambiente de desenvolvimento CODESYS. Nas versões mais recentes, ele já vem pré-instalado. Caso não esteja disponível no seu sistema, siga os passos abaixo para instalá-lo.

Para instalar o complemento, acesse **Tools**  $\rightarrow$  **CODESYS Installer**. Na nova janela aberta, clique em **Browse** e pesquise por **Security**. Em seguida, selecione **CODESYS Security Agent** e clique em **Install**, conforme ilustrado na Figura 3.1 na página 3-1. Antes de instalar novos complementos pelo CODESYS Installer, certifique-se de que o software CODESYS esteja fechado.

CODESYS Installer			- 0
		Add Installati	ion 🗸 🛕
ODES15 04 3.5.19.0			
cation :\Program Files\CODESYS 3.5.19.0\CODESYS		E	Browse St
annel for Setups sleases	Channel for Add-ons  Releases	Update Mode	
Add-ons			
		Install Selected	🛨 Install File(
Installed Browse Updates	<b>▼</b> ● ↓ ↑	Install Selected	▲ Install File(.
Installed Browse Updates CODESYS Security Agent Installed Browse Updates Installed Browse Update	<b>↓</b> ↓ ↑ 1.3.0.0	Install Selected  CODESYS Security Agent  Version: 1.3.0.0	
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>↓</b> ↓ ↑ 1.3.0.0	Install Selected       # CODESYS Security Agent       Version:     1.3.0.0       Description     This package contains the CODESYS Security Agent.	
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>▼<sup>®</sup> ↓ ↑</b> 1.3.0.0	Install Selected       Image: Security Agent       Version:     1.3.0.0       Description     This package contains the CODESYS Security Agent.       Vendor:     CODESYS GmbH	± Install File( Install
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>▼<sup>0</sup> ↓ ↑</b> 1.3.0.0	Install Selected         Image: Code Security Agent         Version:       1.3.0.0         Description       This package contains the CODESYS Security Agent.         Vendor:       CODESYS GmbH         Copyright:       Copyright (c) 2017-2022 CODESYS Development GmbH	± Install File( Install
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>₹<sup>0</sup> ↓ ↑</b> 1.3.0.0	Install Selected         Et CODESYS Security Agent         Version:       1.3.0.0       Image: Colspan="2">Image: Colspan="2"         Colspan="2" Colspan="2"       Colspan="2" Colspa="2" Colspa="2" Colspa="2" Colspan="2" Colspan="2" Colspan="2" Co	± Install File( ▼ Install
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>₹№ ↓</b> ↑ 1.3.0.0	Install Selected	Install File(     Install
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>₹</b> • <b>• • • • • • • • • </b>	Install Selected	Install File(     Install
Installed Browse Updates CODESYS Security Agent CODESYS Security Agent	<b>₹</b> <sup>0</sup> ↓ ↑ 1.3.0.0	Install Selected	Install File(     Install

Figura 3.1: Instalando o complemento CODESYS Security Agent.

# 3.2 RUNTIME CODESYS

As configurações de segurança do runtime do CODESYS podem ser alteradas acessando **Communication Settings**  $\rightarrow$  **Device**  $\rightarrow$  **Change Runtime Security Policy**, conforme ilustrado na Figura 3.2 na página 3-2.

Na seção **Device User Management**, é possível definir o gerenciamento de login do usuário como opcional (**Optional user management**) ou obrigatório (**Enforce user management**). Além disso, a opção **Allow anonymous login** permite estabelecer uma conexão OPC UA sem a necessidade de fornecer credenciais de usuário e senha.



#### NOTA DE CIBERSEGURANÇA!

Recomenda-se não permitir conexões anônimas via OPC UA, pois isso pode expor o sistema a acessos não autorizados e vulnerabilidades de segurança. A OPC Foundation sugere que a autenticação seja feita por meio de login com usuário e senha (**Sign**) ou com autenticação e criptografia (**SignAndEncrypt**).

				Change Runtime Security Pol	icy X
				Communication Current policy New policy	Optional encryption          Optional encryption <ul> <li>Prioral encrypted</li> <li>The device supports both encrypted and unencrypted communication.</li> <li>This can be decided by the user.</li> </ul>
Communication Settings	Scan Network Gate	way 👻 D	Device -	Code Signing	
Applications		_	Options	Current policy	All
			Rename Active Device	New policy	All
Backup and Restore		ы	Wink Active Device		All types of application code accepted.
Files			Forward Communication		
Log			Change Runtime Security Policy	Device Liser Management	
DI C Cattinga			Security Settings	Current policy	Optional user management
PLC Settings			IP-Address: localhost	New policy	Enforced user management
PLC Shell			Port:		The user management on the device is active and cannot be disabled by the user.
Users and Groups			1217		
Access Rights					Allow anonymous login     If anonymous login certain conjutered components (e.e., OPC UA) can
Symbol Rights					establish a connection without providing credentials even if user management is enabled.
Licensed Software Metrics					
IEC Objects					OK Cancel

Figura 3.2: Acessando configurações de segurança do runtime do CODESYS.

#### NOTA DE CIBERSEGURANÇA!

A

O CODESYS oferece diversas funcionalidades de segurança, incluindo criptografia na comunicação entre o runtime e o PLC, controle de acesso à aplicação por usuários, autenticação baseada em certificados, proteção contra manipulação de código-fonte, assinaturas digitais para aplicações, entre outras. Essas medidas garantem maior proteção contra acessos não autorizados e manipulações indevidas. Para mais informações, consulte a ajuda online em CODESYS Online Help.

Caso a opção **Enforce user management** esteja habilitada, será necessário fornecer credenciais para estabelecer a conexão do Cliente com o Servidor OPC UA. Se nenhum usuário estiver configurado no PLC, na próxima tentativa de login, o sistema solicitará a criação de um novo usuário e senha, conforme ilustrado na Figura 3.3 na página 3-2.

	Add Device User	×
CODESYS	Name Default group	WEG Administrator
The mandatory use of the user management is configured for the device. This means that in order to connect to the device an activated user management must be available. Currently, the user management is not activated on the device. Would you like to activate it now? Please note: When activating the user management you will be asked to create a new admin user. Then you will be asked to login as this user.	Password Confirm password Password strength Password policy	
Sim Não		K Cancel

Figura 3.3: Configuração obrigatória de usuário para fazer login no PLC.

#### NOTA DE CIBERSEGURANÇA!

Sempre utilize senhas fortes ao realizar login no PLC, combinando letras maiúsculas e minúsculas, números e caracteres especiais. Durante o comissionamento, altere quaisquer senhas padrão existentes e estabeleça uma política de trocas regulares para reforçar a segurança do sistema.

Se o usuário e/ou a senha para login no PLC forem esquecidos, o acesso ao dispositivo pode ser recuperado por meio do **Factory Reset**, que restaura as configurações de fábrica do produto. Essa funcionalidade está disponível por meio da página web, do PLC Shell no CODESYS e também através do SmartMedia. Para mais detalhes, consulte os manuais dos produtos, disponíveis no site da WEG.



#### ATENÇÃO!

Ao realizar a restauração dos dados de fábrica, **todas as aplicações do CODESYS**, logs, arquivos armazenados no PLC e configurações de rede serão apagados. O produto será reiniciado automaticamente após a conclusão dessas operações.

# 3.3 CONFIGURAÇÕES DE SEGURANÇA DO OPC UA

As configurações de segurança do Servidor OPC UA podem ser visualizadas em **Communication Settings**  $\rightarrow$  **Device**  $\rightarrow$  **Security Settings**, conforme mostra a Figura 3.4 na página 3-3. Nesta janela, pode-se alterar a política de segurança utilizada para autenticação da comunicação entre o Cliente e Servidor OPC UA.



Figura 3.4: Acessando as configurações de segurança do PLC500.

Através do ícone + no **CmpOPCUAServer**, tem-se as possíveis configurações de segurança e informações do Servidor OPC UA, de acordo com a Figura 3.5 na página 3-3.

Device Security Settings		×				
Setting	Value	Description				
😑 🚞 CmpOPCUAServer						
CommunicationPolicy	POLICY_AES128SHA256RSAOAEP	Support for all policies beginning with Aes128Sha256RsaOaep (AES 128 with SHA256)				
Communication Mode	SECURE_IF_POSSIBLE	Support all available modes, but deactivates None if it is possible to use secure endpoints (e.g. certificates created).				
Activation	ACTIVATED	Activates the OPC UA Server. [Default]				
<ul> <li>UserAuthentication</li> </ul>	ENABLED	Activates the user authenticaiton for the OPC UA Server. [Default]				
Allow UserPasswordOn Plaintext	NO	Forbids to tramsit the password in a plaintext way.				
EnableCRLChecks	YES	Enable CRL checks. Verification will fail, if CRL for a CA are missing.				
Enable Self SignedCert Backward Interoperability	YES	Enable backward interoperability.				
CreateWithCAFlag	NO	Configuration to create self signed certificates with cA:FALSE as proposed by the RCFs for non CA certificates. (more secure).				
DeactivateSecurityPolicy		A comma sperated list of security policies uris (e.g. http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256) which needs to b				
ApplicationName	OPCUAServer@PLC500	The application name of the OPC UA server. This will be used for the certificate and the ApplicationName fields of the OPC UA Server.				
CompanyOrOrganizationName		The name of the organization running the OPC UA server. (If empty field is ignored)				
🔦 City		Will fill up the city field of the OPC UA Server certificate. If empty the field won't be used.				
🔧 State		Will fill up the state field of the OPC UA Server certificate. If empty the field won't be used.				
🔦 Country		Country field of the OPC UA Server certificate in alpha-2 code format according to ISO-3166 (e.g. DE for Germany). If empty the field wo				
CertificatelpAddresses		A comma sperated list of IP addresses which should be added as alternative names to the X.509 certificate of the OPC UA Server. Spec				
🗉 🧰 CmpOpenSSL						
🗉 📴 CmpUserMgr						
표 🚞 СтрАрр						
🗉 📴 CmpSecureChannel						
🗉 🚞 CmpWebServer						
		OK Cancel				



O campo **CommunicationPolicy** define a política de segurança suportada pelo Servidor OPC UA. As políticas disponíveis são: Aes256Sha256RsaPss, Basic256Sha256 e Aes128Sha256RsaOaep. A OPC Foundation recomenda a utilização, no mínimo, da política Basic256Sha256. Algoritmos de criptografia desatualizados, que utilizam SHA-1, não devem ser empregados.

Em **CommunicationMode**, é possível configurar o modo de conexão permitido pelo Servidor OPC UA. Recomenda-se utilizar a opção MIN\_SIGNED, a qual exige sempre usuário e senha.

# 

Para quebrar uma encriptação AES-128 por força bruta, seriam necessárias  $2^{128}$  combinações. Com um supercomputador capaz de realizar  $1 \times 10^{18}$  operações por segundo, o tempo estimado para a tarefa seria de até  $10, 8 \times 10^{12}$  (trilhões) de anos.

Para mais informações sobre as opções de segurança do OPC UA, consulte a ajuda online em CODESYS Online Help.

# 3.4 CRIAÇÃO DE CERTIFICADO AUTOASSINADO

Para criar um certificado autoassinado, acesse **View**  $\rightarrow$  **Security Screen** ou clique no ícone @, localizado no canto inferior esquerdo da janela do CODESYS, conforme ilustrado na Figura 3.6 na página 3-4.

Na janela que se abrirá, selecione a aba **Devices**, clique no ícone de atualização  $\diamondsuit$  e, em seguida, clique no ícone **Device** para visualizar os certificados disponíveis, conforme demonstrado na Figura 3.7 na página 3-4.



Figura 3.6: Abertura da tela de segurança no CODESYS.

🔇 Security Screen 🗙									-
User	Φ	Information	1	*	Information	Issued for	Issued by	Valid from	Valid until
Designation	1	🖃 🔟 Device	2	ĸ	Redundancy (not available)				
Project		Own Certificates	4		OPC UA Server (not available)				
Devices		Trusted Certificates	0	10	Encrypted Application (not available)				
benes		Untrusted Certificates	Q		Encrypted Communication	PLC500	PLC500	20/02/2025 11:57:19	22/03/2025 11:57:19 (30 days)
		Quarantined Certificates	ſ	*	Web Server (not available)				
				*					

Figura 3.7: Tela de certificados do dispositivo.

Para criar um novo certificado, acesse **OPC UA Server** e clique no ícone <sup>1</sup>. Em seguida, escolha o tamanho da chave, defina a validade do certificado e clique em **OK**.

Aguarde a geração do certificado — quanto maior o tamanho da chave, mais seguro será o certificado, porém o processo de criação levará mais tempo. Após a conclusão, o certificado poderá ser visualizado conforme ilustrado na Figura 3.8 na página 3-5. Além disso, os certificados criados pelo PLC500 podem ser listados diretamente via PLC Shell, utilizando o comando **cert-getcertlist**.



A

# NOTA!

O certificado utilizado para a encriptação da comunicação entre o CODESYS no computador e o PLC é gerado automaticamente, dispensando a necessidade de criação 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: Novo certificado Servidor OPC UA gerado no CODESYS.

#### NOTA DE CIBERSEGURANÇA!

Os certificados gerados pelo CODESYS não possuem a autenticidade de uma Autoridade Certificadora (CA), portanto, qualquer Cliente OPC UA que desejar realizar uma comunicação segura deve reconhecer manualmente o certificado gerado.

# 4 SERVIDOR OPC UA - CODESYS

Esta seção apresenta um exemplo de configuração de um Servidor OPC UA no CODESYS utilizando o PLC500.

Inicialmente, adicione o Symbol Configuration à aplicação: clique com o botão direito em Application  $\rightarrow$  Add Object  $\rightarrow$  Symbol Configuration, conforme ilustrado na Figura 4.1 na página 4-1. Marque a opção Support OPC UA features option e clique em Add.



Figura 4.1: Adicionando o Symbol Configuration à aplicação no CODESYS e habilitando os recursos OPC UA.

Em seguida, em **Symbol Configuration**, clique em **Build**. Os símbolos serão criados para todas as variáveis declaradas no projeto. Para selecionar os dados a serem disponibilizados pelo Servidor OPC UA, habilite as caixas **Z** clicando com o botão esquerdo na lista de **Symbols**, como demonstrado na Figura 4.2 na página 4-1.

Symbol Configuration 🗙						-
📉 View 👻 🛗 Build 🛛 🛱 Settings 👻	Tools 👻					
Changed symbol configuration will be tra	ansferred with the next	download or	online chang	e		
Symbols	Access Rights	Maximal	Attribute	Туре	Members	Comment
🖭 🗐 📄 Constants						
🖲 🔲 📄 IoConfig_Globals						
🗉 🔲 📄 IoConfig_Globals_Mapping						
🖻 🔽 📄 PLC_PRG						
war_BOOL	Star 1	<b>*</b>		BOOL		
🐨 🔽 🛷 var_DWORD	Star 1	<b>*</b>		DWORD		
🐨 🔽 🛷 var_REAL	×>	<b>*</b>		REAL		
🛛 🕼 🔷 var_USINT	<b>*</b>	<b>*</b>		USINT		
war_USINT	7	V		USINI		

Figura 4.2: Configuração de variáveis no Symbol Configuration.



#### NOTA!

Por padrão, as variáveis possuem direitos de acesso para leitura e escrita pelo Cliente OPC UA, como observado na variável **var\_DWORD**, indicada pelo ícone \*. As variáveis com acesso apenas de leitura possuem o ícone \*, enquanto aquelas com acesso apenas de escrita possuem o ícone \*. Para modificar o tipo de acesso, clique com o botão esquerdo sobre os ícones.

# 5 CLIENTE OPC UA - UA EXPERT

Esta seção apresenta um exemplo de configuração de um Cliente OPC UA no **UAExpert**<sup>®</sup>. O programa está disponível para download no site da Unifed Automation.

# 5.1 ENCONTRANDO SERVIDORES PELO URL

No UAExpert, clique no ícone + para adicionar um Servidor OPC UA. Em seguida, dê um duplo clique no + do **Custom Discovery** e digite o URL correspondente ao IP do seu Servidor OPC UA. Por exemplo, se o IP for 192.168.1.10, a URL será **opc.tcp://192.168.1.10:4840**. A Figura 5.1 na página 5-1 mostra os passos para adicionar o Servidor OPC UA no UAExpert.

File View Server Document Set	tings Help	
🗅 💋 🕞 🔀 💽	🔶 — 🜣 🗙 🔧 💄 🖻 🕱 🗖	
Project	Add Server	? ×
✓ 📁 Project	Enter URL ? X	
D Servers	Configuration Name  Enter the URL of a computer with discovery service running:	
∨ 📁 Documents	PKI Store Default opc.tcp://192.168.1.10:4840	$\sim$
📁 Data Access View	Discovery Advanced OK Cancel	
	Endpoint Filter: No Filter	$\sim$
	Q Local	1
	> 🔍 ServersOnNetwork	
	V 🚱 Global Discovery Server	
	Couble click to Add GDS Server >	
Address Space	✓ See Custom Discovery	
	A state of the	
	✓	

Figura 5.1: Adição do Servidor OPC UA no UAExpert.

Em seguida, clique na URL e expanda os ícones até que as conexões disponíveis sejam exibidas. Dependendo da configuração de segurança do Servidor OPC UA do PLC500, nem todas as opções estarão visíveis. Utilize as opções de conexão que apresentarem um Endpoint URL com o endereço IP do Servidor OPC UA do PLC500, como mostrado na Figura 5.2 na página 5-1. Endpoints URL com o nome do host gerarão um erro de conexão.



Figura 5.2: Todas as opções de conexão Servidor OPC UA do PLC500 no UAExpert.



# NOTA!

Para que todas as opções de conexão apareçam no UAExpert, um certificado autoassinado para o OPC UA precisa ser criado no PLC500. Além disso, o **CommunicationMode** deve estar configurado para **ALL**. Confira a Seção 3 CONFIGURAÇÕES DE SEGURANÇA na página 3-1 para mais informações.

# 5.2 CONEXÃO ANÔNIMA

a.

Para que uma conexão anônima seja possível, é necessário habilitar a opção Allow anonymous login em Change Runtime Security Policy e configurar CommunicationMode para ALL em Device Security Settings.



#### NOTA DE CIBERSEGURANÇA!

A utilização de conexão anônima para a operação regular de aplicações não é recomendada devido a questões de cibersegurança. Ela deve ser restrita a fins de teste, comissionamento ou quando outras alternativas não estiverem disponíveis.

Selecione a opção de conexão **None** e clique em **OK**, conforme Figura 5.3 na página 5-2. O Servidor OPC UA aparecerá abaixo da pasta **Servers**. Clique com o botão direito e selecione **Connect**, ou clique no ícone correspondente na barra de ferramentas, conforme mostrado na Figura 5.4 na página 5-2.

Add	Server			?	×
Configur	ration Name	OPCUAServer@PLC500			
PKI Sto	re	Default			$\sim$
Disco	very Ad	lvanced			
Endp	oint Filter:	No Filter		```	~
	🔍 L	ocal			
>	🔍 S	erversOnNetwork			
~	🖌 💽 G	lobal Discovery Server			
	_ <b>4</b>	Souther state of the second			
~	🗸 🗺 c	ustom Discovery			
	¢	Souther state of the second server >			
	<b>~</b> (	🔪 opc.tcp://192.168.1.10:4840			
	`	<ul> <li>OPCUAServer@PLC500 (opc.tcp://192.168.1.</li> </ul>	10:4840)		
		📔 None - None (uatcp-uasc-uabinary)			
		None - None (uatcp-uasc-uabinary)			
~	🗸 💽 R	everse Discovery	Endpoint URL: opc.tcp://192.168.1.10:4840 Security Policy: None		
	q	Souther state of the second	Message Security Mode: None Security Level: 0		1
>	🛛 🚫 Re	cently Used		_	
	Authenticati	on Settings maus			

Figura 5.3: Selecionando a comunicação sem encriptação.

[		Ø	₿	Ø	0	•	-	0	*	2		R	
Proje	ect							ረ እ					
~		Proje	ect										
	~		Servers										
		-		UAServ	er@PLC500	)	Connect	:	H				
	Ŷ	-	Documer Documer	a Acce	ss View	2	Disconn	ect					
			0			2	Change	User					
						-	Remove						

Figura 5.4: Estabelecendo conexão com Servidor PLC500 OPC UA no UAExpert.

A conexão será estabelecida, e as variáveis acessíveis estarão presentes em **Objects**  $\rightarrow$  **DeviceSet**  $\rightarrow$  **PLC500 Industrial**  $\rightarrow$  **Resources**  $\rightarrow$  **Application**  $\rightarrow$  **Programs**. Essas variáveis podem ser selecionadas e arrastadas para a janela **Data Access View**, onde poderão ser monitoradas em tempo real, conforme mostrado na Figura 5.5 na página 5-3.



Figura 5.5: Monitoração das variáveis no UAExpert.

#### 5.3 CONEXÃO SEGURA

Para estabelecer uma conexão segura OPC UA com o Servidor do PLC500, é necessário configurar previamente um usuário e um certificado no PLC. Para mais detalhes, consulte a Seção 3 CONFIGURAÇÕES DE SEGURANÇA na página 3-1.

Selecione uma opção de segurança com credenciais (**Sign**) ou com credenciais e criptografia (**SignAndEncrypt**). Clique no ícone correspondente para habilitar a autenticação, insira o usuário configurado no PLC500, conforme mostrado na Figura 5.6 na página 5-3, e clique em **OK**.

onfiguration Name	OPCUAServer@	PLCS00	
(I Store	Default		
Discovery Ad	vanced		
Endpoint Filter:	No Filter		$\sim$
	2	None - None (uatcp-uasc-uabinary)	
		Aes128_Sha256_RsaOaep - Sign & Encrypt (uatcp-uasc-uabinary)	
	Ø	Aes128_Sha256_RsaOaep - Sign (uatcp-uasc-uabinary)	
	<u></u>	Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)	
		Basic256Sha256 - Sign (uatcp-uasc-uabinary)	
		Aes256_Sha256_RsaPss - Sign & Encrypt (uatcp-uasc-uabinary)	
		Aes256_Sha256_RsaPss - Sign (uatcp-uasc-uabinary)	
Authenticatio	n Settings		
Anonyr	nous		
line			
Oserna	ine	weg Sure	
Passw	ord		
Certifi	ate		
Private	e Key	m	

Figura 5.6: Selecionando uma conexão OPC UA segura no UAExpert.

O Servidor OPC UA aparecerá abaixo da pasta **Servers**. Clique com o botão direito sobre ele e selecione **Connect**, ou utilize o ícone correspondente na barra de ferramentas. Na janela que se abrir, insira a senha do usuário configurado e confirme.

	Ø		2	0	ф	-	\$	×	2	2	E	R	Enter u	iser credentials	?	×
Project							ረን									
~ <b></b>	Proje	ct Servers					U						Please enter to the serve	r the user credentials r 'OPCUAServer@	for the con PLC500	nection '
		🔕 opc	UAServe	er@PLC500	5			_					Username:	weg		
~		Docume	nts		-	Connect										
		-			20	Disconne	ect						Password:	•••		
		Dat	ta Acces	s View	4	Propertie	es									
					2	Change	User							OK	Carr	-
					-	Remove									Carro	
					_											

O aviso **BadCertificateHostNameInvalid** ocorre quando o nome do host no certificado do Servidor OPC UA não corresponde ao endereço utilizado para a conexão, como ao usar um IP em vez de um nome de domínio. Caso o certificado seja confiável e o usuário saiba da sua origem, o aviso pode ser ignorado.

Após clicar em **OK**, será exibida uma janela para confiar no certificado do PLC500. Clique em **Trust Server Certificate** e, em seguida, clique em **Continue** para finalizar o processo de confiança e estabelecer a conexão segura. A Figura 5.7 na página 5-4 mostra as telas de validação de certificado do UAExpert.

Validating the certific	cate of server 'OPCUAServer@PLC500' returned a	an error:	The certificate of server '	OPCUAServer@PLC500' was validated succe	essfully.
BadCertificateU	ntrusted	♥	Good		
rtificate Chain		c	ertificate Chain		
Name	Trust Status		Name	Trust Status	
S OPCUASe	rver@PLC500 Untrusted		A OPCUAServer	@PLC500 Trusted	
rtificate Details			ertificate Details		
rrors Error	ok [BadCertificateUntrusted]	1	Subject Common Name	OPCUAServer@PLC500	_
Common Nan	ne OPCUAServer@PLC500		Organization OrganizationUnit		
Organization	Jnit		Locality		
Locality			State		
State			DomainCompone	nt	
Country			Issuer		_
DomainComp	onent		Common Name	OPCUAServer@PLC500	
Ssuer			Organization		
	ne OrcoAserver@PLC500		OrganizationUnit		
	T	Trust Server Certificate		т	rust Server Certifica

Figura 5.7: Validação do certificado pelo UAExpert.

No CODESYS, vá para a **Security Screen** e verifique se o certificado do Cliente OPC UA do UAExpert está na quarentena. Arraste-o para a pasta **Trusted Certificates** para adicioná-lo à lista de certificados confiáveis.

💱 Security Screen 🗙								•
User	Φ	Information	E#	Information	Issued for	Issued by	Valid from	Valid until
Deviant	-	🖻 🔟 Device	X	<b>₩</b>	UaExpert@BRJGSTER276432	UaExpert@BRJGSTER276432	05/02/2025 16:20:44	05/02/2027 16:20:44 (> 1 year)
Project		Own Certificates	121					
Devices		Trusted Certificates						
		Untrusted Certificates	h					
		Quarantined Certificates	12					

O certificado do UAExpert deve aparecer agora na janela de certificados confiáveis.

Security Screen X								
User	Φ	Information	1	Informati	on Issued for	Issued by	Valid from	Valid until
Project	1	Device	×	<b>1</b>	UaExpert@BRJGSTER276432	UaExpert@BRJGSTER276432	05/02/2025 16:20:44	05/02/2027 16:20:44 (> 1 year)
		Own Certificates     Trusted Certificates	1					
Devices		Untrusted Certificates						
		Quarantined Certificates	Ē#					

NOTA!

Todos os certificados criados e confiáveis do PLC500 podem ser também visualizados através do comando **cert-getcertlist** no PLC Shell.

Após reconectar o Servidor OPC UA no UAExpert, a conexão deve ser estabelecida corretamente. As variáveis localizadas em Tags  $\rightarrow$  Objects  $\rightarrow$  DeviceSet  $\rightarrow$  PLC500 Industrial  $\rightarrow$  Resources  $\rightarrow$  Application  $\rightarrow$  Programs podem ser arrastadas para a janela Data Access View, permitindo que as variáveis sejam lidas ou modificadas conforme necessário.





# NOTA!

Quando um certificado é confiado permanentemente, ele pode ser utilizado para estabelecer outras conexões seguras no UAExpert até que sua data de validade expire.

# 6 CLIENTE OPC UA - WES

Esta seção apresenta um exemplo de configuração de um Cliente OPC UA no **WES (WEGnology Edge Suite)**. Para acessar a página do WES, visite o site da WEG.

#### 6.1 SOBRE O WES

A plataforma WEGnology Edge Suite é um moderno e avançado software supervisório para controle e automação de processos industriais e desenvolvimento de aplicações IoT na borda.

O WES é uma solução completa, segura, flexível e escalável desde aplicações HMI até avançados sistemas SCADA, centros de controle e supervisão de processos industriais distribuídos de missão crítica e alta disponibilidade, incluindo versão WES-ELECTRICAL para sistemas elétricos possibilitando a aplicações nos mais diversos segmentos da Indústria incluindo fabricantes de máquinas e equipamentos (OEMs).



# 6.2 CRIAÇÃO DO PROJETO

No WES, crie um novo projeto em **Projects**  $\rightarrow$  **New Project**. Também é possível verificar a licença atual do WES em **License**. A Figura 6.1 na página 6-1 apresenta a tela inicial do WES.



Figura 6.1: Tela inicial do WES.

Uma vez dentro do projeto criado, é apresentada a Figura 6.2 na página 6-2, onde são encontrados os campos principais **Edit**, **Draw** e **Run**.

CPCUA-PLC500			— C	) X
OPCUA-PLC500		· 유니크 슈니티, 아,   양 반 왕		0
Edit Draw Run Info	Current Project Version Editing with from	Redundancy       Im: Build 0 on 09/05/2024 12:43:15       th: WEGnology EDGE Suite wd-9:2.56       m: Local computer		
Soffrack	OPCUA-PLC500 Project Title: Description: Total Tags:	OPCUA-PLC500		<u> </u>
Help	Project Path: Project Type: File Extension: Project Example: Protocols:	G CWREGnologyEDGESuite\Projects\ Current tproj		
License	Last Opened: TargetFramework: Product Version: Product Family: Product Model: Product Path: Schema Version: Preview:	09/05/2024 13:20:10 .NET Framework 4.6.2 wd-9.2.56 WES Machine CAProgram Files (x86)\WEG\WEGnologyEDGESuite\wd-9.2\ 2019.2.27		
WEGnology EDGE Suite wd-9.2.56	Find window	OnlineConfig disconnected	Соруг	ight by WEG

Figura 6.2: Tela inicial do projeto.

Vá em Edit  $\rightarrow$  Devices  $\rightarrow$  Channels e escolha o OPCUA - OPC UA Client em Installed Protocols. Em seguida, clique em Channel: Create new e Ok para criar um novo canal. A Figura 6.3 na página 6-2 mostra o canal OPC UA criado.

🚔 OPCUA-PLC500						- 0	×
<b>O</b> D-							
OPCUA-PLC500	णहते 🔊 🔄 ्र छ	🕮 🖂 🔂 🗟 🧠 ServerMo	nitorlr 📖 😵 📮 🛞				0
🗱 🏪 💽 🕕	Channels	lodes Points	AccessTypes				
Tags	Installed Protocols:	OPCUA - OPC UA Client	- He	lp			
	Channel:	Create new					
Security	Drag a column heade	r here to group			Filter by Na	me:	0-
Devices	Name	Protocol ProtocolOptions	Interface Settings	Timeout	InitialState	Description	
		OPC_UA	Custom			OPCUA - OPC UA Client	- 1
Alarms							
Datasets							
Scripts							
Displays							
Leports							
WEGnology EDGE Suite wd-9.2.56	Find window		OnlineConfig disconned	ted		Соругід	ht by WEG

Figura 6.3: Criando um novo canal.

Para criar um novo nó, vá em Edit  $\rightarrow$  Devices  $\rightarrow$  Nodes  $\rightarrow$  New e clique em Ok. Na mesma janela, clique no campo em branco em PrimaryStation para abrir a seta à direita. Clique na seta para abrir o configurador.

A OPCUA-PLC500 weg Filter by Name: Drag a column header here to gr Channel PrimaryStation Name BackupStation Description Devices OPC\_UA OPC\_UA OPC UA - Endpoint B 192.168.234.234 Script ch returned 2 Endp URL Security Mode oc.tcp:/

Em **Discovery**, insira o endereço IP da conexão em **IP Address** e clique em **Search**. Selecione o dispositivo e então clique em **Ok**. A Figura 6.4 na página 6-3 mostra as telas para criação do novo nó.

Figura 6.4: Criando e configurando um novo nó.

Na URL da janela **Discovery**, altere o nome do dispositivo para o endereço IP do Servidor OPC UA. Por exemplo, se o IP for 192.168.1.10, a URL ficará **opc.tcp://192.168.1.10:4840**. Depois, clique em **Test**. Se tudo correr bem, a mensagem **Connected** será exibida ao lado do botão **Test**. A Figura 6.5 na página 6-3 mostra o teste para conexão de um novo Servidor OPC UA.



Figura 6.5: Teste e conexão de um novo Servidor OPC UA.

Para selecionar as variáveis de interesse do CODESYS, vá em **Edit**  $\rightarrow$  **Devices**  $\rightarrow$  **Nodes**  $\rightarrow$  **Import**  $\rightarrow$  **Update**. Pode-se selecionar uma única variável, um grupo de variáveis, POUs ou programas inteiros. A Figura 6.6 na página 6-4 mostra a importação de variáveis do Servidor OPC UA.



Figura 6.6: Importando variáveis do Servidor OPC UA.

As variáveis selecionadas anteriormente podem ser visualizadas em Edit  $\rightarrow$  Devices  $\rightarrow$  Points. Suas permissões podem ser modificadas na opção AccessType, alterando entre Read, Write ou ReadWrite. A Figura 6.7 na página 6-4 apresenta a tela de alteração de permissões de acesso.

📸 OPCUA-PLC500									-		×
OPCUA-PLC500	III 🧐 😋 👗 🗈 🏔 😫	\$ <u>, </u>	n_var_PLC500_Ir	👻 📮	* *						0
🗱 🏣 💽	Channels Nodes	P	Dints AccessTy	pes							
	Drag a column header here to	group				Fi	lter by Addre	255:			
Tags	TagName	Node	Address	DataType	AccessType	Modifiers	Scaling	Label			
Security	n_var_PLC500_Industrial_App	OPC_UA	ns=4;s= var PLC500	Native	Read	]					
Devices					Read ReadWrite	}					
Alarms											
Datasets											
Scripts											
Displays											
Leports											
WEGnology EDGE Suite wd-9.2.56											▼
	Find window		c	nlineConfig o	disconnected				Сор	oyright by	y WEG

Figura 6.7: Alterando permissões de acesso.

As variáveis importadas do CODESYS podem agora ser utilizadas no sistema SCADA. Por exemplo, acesse **Draw**  $\rightarrow$  **Drawing**  $\rightarrow$  **TextBox**. Em seguida, dê um duplo clique na caixa detexto e vá para **TextIO**  $\rightarrow$  **ObjectName**  $\rightarrow$  **Tag**, selecionando a variável apropriada do CODESYS. Na Figura 6.8 na página 6-5 é mostrado como selecionar variáveis do CODESYS para a utilização no WES.



Figura 6.8: Utilizando as variáveis do CODESYS no WES via OPC UA.

 $Em Execute \rightarrow Initialization \rightarrow Execute Initialization$ , é aberta a janela mostrada na Figura 6.9 na página 6-5, onde as variáveis OPC UA da aplicação podem ser monitoradas.

💕 Startu	p Window			_		×
File Tool	s Security			 _	11-39-34	
<b>*</b> 0		Project: OPCUA-PLC500	SUEST	•	20/05/2024	۲
var1						
1,00						
var2						
3,00						
				-		

Figura 6.9: Monitoração das variáveis OPC UA.

# 7 CLIENTE OPC UA - EASY BUILDER PRO

Esta seção apresenta um exemplo de configuração de um Cliente OPC UA no Easy Builder PRO utilizando uma IHM cMT2078X. O programa pode ser baixado no site da Weintek.

Para começar, crie um novo projeto no Easy Builder PRO acessando File  $\rightarrow$  New Project, selecione o modelo da sua IHM e clique em **Ok**.

# 

Atualmente, os modelos de IHM da WEG que suportam Cliente OPC UA são MT8051iP, MT8072iP, cMT2078X, cMT1106X e cMT2108X2. Para mais informações, consulte a página do produto no site da WEG.



Em seguida, a janela **System Parameter Settings** será aberta. Adicione um novo dispositivo em **New Device/Server**. Em **Device Type**, selecione **OPC UA Client**. A interface **I/F:** deve estar configurada como **Ethernet** por padrão. Clique em **Settings** e defina o endereço IP.

	Device Settings
	Name : OPC UA Client
	O Device
	Location : Local Settings * Select Local for a device connected to this HMI, or Remote for a device connected through another HMI.
ystem Parameter Settings X	Device type : OPC UA Client
Time Sync./DST e-Mail FTP	Device ID : 373, V.5.30, WEINTEK_OPCUA_CLIENT.c33
Device Model General System Remote Security Extended Memory Cellular Data Network	I/F: Ethernet  V Open Device Connection Guide
Device list: What's my IP?	
Name Location Device Type Interface I/F Protocol Station No.	
	IP : [192.168.1.111, Port=4840 Settings
New HMI Delete Settings/Security	
Settings made in this tab will be saved directly (no cancel)	
* HMI doesn't support CAN bus if CODESYS feature is activated.	
* Add a [Weintek Built-in CODESYS] device to communication with Built-in CODESYS.	OK Cancel

# 7.1 CONEXÃO ANÔNIMA

Para que uma conexão anônima seja possível, é necessário habilitar no CODESYS o **Allow anonymous login** em **Change Runtime Security Policy**. Além disso, a **CommunicationMode** deve estar configurada como **ALL** para o **CmpOPCUAServer** em **Device Security Settings**. Confira a Seção 3 CONFIGURAÇÕES DE SEGURANÇA na página 3-1 para mais informações.



NOTA DE CIBERSEGURANÇA!

A utilização de conexão anônima para a operação regular de aplicações não é recomendada devido a questões de cibersegurança. Ela deve ser restrita a fins de teste, comissionamento ou quando outras alternativas não estiverem disponíveis.

Após ter configurado o IP do Servidor OPC UA no PLC500, clique em Security, Authentication.

Device Settings			
IP Address Settings			
IP address	: 192 . 168 . 1	. 10	
Port no.	: 4840		
	Security, Authenitcati	ion	
	,		
Communication Settings			
Timeout (se	c): 5.0 •		
Turn around delay (m	s): 0		
Resending command	ds : 0 •		

Na janela **OPC UA Advanced Settings**, clique no ícone **a**. Clique em **Search** para detectar os servidores disponíveis no endereço IP configurado. Selecione uma das opções de conexão anônima em **None** e clique em **Apply**. Mantenha o restante das configurações padrão e clique em **Ok** para fechar as janelas até voltar ao **System Parameter Settings**.

OPC UA Advanced Settings				
Endpoint url : opc.t Server name :	cp://192.168.1.10:4840		Discover Server	
Security Security policy : None Message security mode : None Re-build Certificate when HMI star Support Uncertain Initial Value Trusted Server Certificate : Authentication	ts Import	~	opc.tcp://192.168.1.10:4840 • opc.tcp://192.168.1.10:4840 • OPCUAServer@PLCS00 • None - None • None - None	Sear
Anonymous			Арріу	Exi

Selecione o **OPCUA Client** e clique em **Tag Manager**. Selecione uma das opções de mapeamento das variáveis e clique em **Ok**.

System Parameter Settings	×	<										
Cellular Data Network Printer/Backup Server Time Sync./DST Device Model General System Remote Security	e-Mail Extended Memory		IEC-61131 STRIN	G type selec	t							×
Device list:           Name         Location         Device Type         Interface           Local HMI         Local         MT8071IP / MT8071IP2 / MT8072IP (800 x 480) -           Local D         OPC U         Local         OPC UA Client	What's my IP? I/F Protocol Stati - 0 TCP/IP N/A		The XML imported Please select your p	contains IEC-6 xreference.	1131 STRING ty	pe. In EasyBuild	erPro, IEC-6113	I STRING type is hand	led in one of	the following wa	iys.	
			One char p Each single-byte WORD's high b E.g. The 4-chara	er word character is n /te is zero-pad cter string "AB	napped to a WO ded. CD* is mapped t	RD in memory. o 4 words.	The	<ul> <li>Two char per</li> <li>Every two characters</li> <li>the first characters</li> <li>high byte.</li> <li>E.g. The 4-characters</li> </ul>	r word tters are map r takes the lo tter string "AB	ped to a WORD w byte, and the s CD* is mapped	in memory. In th second one takes to 2 words.	is case, ; the
			Byte Index Value Character	0 0x41 "A"	1 0x42 "B"	2 0x43 °C*	3 0x44 "D"	Byte Index Value Character	0 0x41 "A"	1 0x42 "B"	2 0x43 "C"	3 0x44 "D"
New Device/Server         Delete           Tag Manager         Import Tags         Export Tags	Settings		Word Index Value	0 0x0041	1 0x0042	2 0x0043	3 0x0044	Word Index Value	0x4	241	1 0x44	443
* Settings made in this tab will be saved directly (no cancel)												ОК

Na janela **Device Address Manager**, verifique se as opções **Addresses** e **Log** estão habilitadas para visualização em **Window**. Clique na seta ao lado de **Device**. Uma janela para aceitar um certificado será aberta. Clique em **Accept Temporarily**.

	Certificate Validation
Device Address Manager	Do you want to trust this server certificate?
File Device Window	Subject
Addresses V Device	Ø ×     Common Name       Organization     OrganizationUnit       Locality     State       Country     DomainComponent       Immer     Common Name       OrganizationUnit     Locality       State     Common Name       OrganizationUnit     Locality       State     Country       DomainComponent     Videty

A conexão anônima com o Servidor OPC UA no PLC500 será estabelecida. Clique sucessivamente na seta em **Object** → **DeviceSet** → **PLC500 Industrial** → **Resources** → **Application** → **Programs**. Todas as variáveis encontradas nos programas do projeto CODESYS serão exibidas. No exemplo, o projeto possui apenas um POU chamado **PLC\_PRG**. Clique na seta ao lado do programa para visualizar as variáveis disponíveis para importação no projeto da IHM. Arraste individualmente cada variável para a janela ao lado.

III Device Address Manager					- 0 X
File Device Window					
Addresses		ē×	Search		Paret
✓ Device					Neset
✓ Objects			Name *	Туре	Full Name
> Server(2253)			var LISINT	BYTE	Objects DeviceSet PIC500 Industrial Resources Appli
✓ DeviceSet			var_obiiti	DITE	objects.bevicesett eesoo muustutatesources.vppil
DeviceFeatures			var_REAL	REAL	Objects.DeviceSet.PLC500 Industrial.Resources.Appli
<ul> <li>PLC500 Industrial</li> </ul>			DWORD	UDINT	
✓ Resources			var_DWORD	UDINI	Objects.DeviceSet.PLC500 Industrial.Resources.Appli
✓ Application			var BOOL	BOOL	Objects.DeviceSet.PLC500 Industrial.Resources.Appli
> GlobalVars	(appo/PLC500 Industrial.Application.GlobalVars)		-		
✓ Programs					
✓ PLC_PF					
Va	-BOOL				
Va	_DWORD				
Val		_			
Tacke(Japp	olPLC500 Industrial Application Tasks)	_			
/ lasks(labb		Ŧ			
Log					e ×
Level Timestamp			Message		
Info 08:32:20.568	server certificate is acceppted temporarily				
Info 08:32:20.587	connection status changed to Connected				
Info 08:32:20.587	succeeded to connect				

Depois de indexar todas as variáveis de interesse do projeto, vá em File  $\rightarrow$  Save e depois File  $\rightarrow$  Exit. Com as tags importadas, clique em Ok na janela System Parameter Settings.

Adicione os objetos desejados na sua interface e associe-os às variáveis do Servidor OPC UA do PLC500 clicando em Tags. Clique sucessivamente nos ícones Tags  $\rightarrow$  Objects  $\rightarrow$  DeviceSet  $\rightarrow$  PLC500 Industrial  $\rightarrow$  Resources  $\rightarrow$  Application  $\rightarrow$  Programs, e selecione o POU associado à variável a ser mapeada.

New Toggle Switch/Bit Lamp	Ĉ.	📲 Objects 📲 DeviceSet 📲 PLC500 Industrial 📲 R	esources 📲 Application 📲 Programs 📲 Pl	.c_prg •
General Security Shape Label	0,	Y 🗎 Tags	Name	Data type Description
Comment :		<ul> <li>✓ <sup>¶</sup> Objects</li> <li>✓ <sup>¶</sup> DeviceSet</li> </ul>	var_BOOL	BOOL ns:4;s: var PLC500 Indu
		<ul> <li>✓ <sup>1</sup>% PLCS00 Industrial</li> <li>✓ <sup>1</sup>% Resources</li> <li>✓ <sup>1</sup>% Application</li> <li>✓ <sup>1</sup>% Application</li> <li>✓ <sup>1</sup>% PLC_PRG</li> <li>Show description</li> </ul>		
		Tag : var_BOOL (ns:4;s: var PLC500 Industrial.Application.P	LC_PRG.var_BOOL)	Ok

Depois de concluir o projeto da IHM com todas as variáveis de interesse, compile o projeto em **Compile** e carregue o programa para a IHM em **Download (PC**  $\rightarrow$  **HMI)**. A imagem a seguir mostra o monitoramento online das variáveis no CODESYS e no Easy Builder Pro através da **Online Simulation**.

PLC_PRG X						
Device.Application.	PLC_PRG					
Expression	Туре	Value	Prepared value	Address	Comment	
var_BOOL	BOOL	TRUE				
var_USINT	USINT	117				
var_DWORD	DWORD	2323				
var_REAL	REAL	22.33				
OPC UA P Bool variat USINT vari 117 DWORD v 2321 REAL varia 22.33	er ( simulat LC500 Se ble iable ariable able	rver cMT2C	178X Client			*

# 8 CLIENTE OPC UA - PLC500ED

Como destacado no início deste documento, todos os PLCs WEG com CODESYS oferecem suporte ao Servidor OPC UA. No entanto, o **PLC500ED** também conta com a funcionalidade de **Cliente OPC UA**.

# NOTA!

A utilização do protocolo **Cliente OPC UA** é possível apenas no modelo PLC500ED através do container **Edge Agent**. Não é possível utilizar essa funcionalidade via CODESYS.

# 8.1 SOBRE O PLC500ED

O PLC500ED mantém todas as funcionalidades do PLC500, mas com a vantagem adicional de suportar processamento de borda (*Edge Computing*) por meio do container **Edge Agent**. Esse recurso permite a conexão de equipamentos industriais às plataformas de nuvem da WEG, como a **WEGnology** e a **WEG Smart Machine**, possibilitando a implementação de soluções digitais avançadas, como monitoramento remoto, manutenção preditiva e análise de dados em tempo real. Para mais detalhes sobre o produto ou sobre as plataformas, acesso o site da WEG.



# 8.2 CONFIGURAÇÃO RÁPIDA

Seguem os passos básicos para configurar de forma rápida uma aplicação WEGnology através do PLC500ED.

- 1. Criar uma aplicação no site WEGnology e salvar suas credenciais ou obter as credenciais de uma aplicação WEG Digital Solution.
- 2. Conectar o PLC500ED à internet por meio da página web ou do CODESYS.
- 3. Inserir os dados da aplicação na aba Cloud Integration da página web.
- 4. Habilitar o container Edge Agent na aba Docker da página web.
- 5. Verificar se o dispositivo foi reconhecido automaticamente como online na plataforma. Neste momento, o **PLC500ED** estará pronto para realizar o *deploy* da aplicação Cliente OPC UA ou qualquer outro *workflow*.

Com todas as configurações efetuadas da forma correta, a página de estado do PLC500ED deve mostrar que o produto está conectado na internet, com uma aplicação também conectada e com o container Edge Agent rodando, conforme mostra a Figura 8.1 na página 8-2.

Core App Version	2.4.1	Config Mode Local
Firmware Version	1.4.3	Integrator wegnology-1
Board Serial	5A2026884	Client Name PLC500ED-2F:F3:C2
System Time	2025-03-20T14:20:12	Application 67a4986ff0664e164c62bfbc
System Uptime	361 min	Client ID 67dc4c93547750fec4a34df8
Memory Usage	25% 256 MB of 997 MB	Status Connected
Disk Usage	13% 1902 MB of 14449	Last State 2025-03-20T17:13:44
	MB	☐ Force Remove
Internet Status	Connected	
Ping Info	0%, 116 ms	DOCKER INFORMATION
	ORMATION	
ETH1 MAC	00:01:C0:2F:F3:C2	from wnology/edge-agent:1.34.0-alpine
ETH1 IP	192.168.1.10	Memory 11.00%
ETH2 MAC	00:01:C0:2F:F3:C3	
ETH2 IP	192.168.29.57	
USB2 MAC	F6:30:CE:70:22:E8	
USB2 IP	192.168.234.234	

Figura 8.1: Tela de estado do PLC500ED.

Para mais detalhes, consulte a Nota de Aplicação do PLC500ED, disponível no site da WEG.

#### 8.3 OPC UA PING PONG

Este exemplo básico de aplicação utiliza um PLC500ED como Cliente OPC UA e um PLC410 como Servidor OPC UA. A cada 5 segundos, o Cliente lê a variável iVar do Servidor. Se o valor for 1, o Cliente escreve 0 em iVar. Paralelamente, o Servidor, através do CODESYS, também lê iVar. Caso o valor seja 0, o Servidor escreve 1 em iVar e incrementa iCount.



NOTA!

A interface ETH1 do PLC500ED deve estar conectada à interface ETH do PLC410.

#### 8.3.1 Servidor OPC UA - PLC410

O PLC410 deve estar com a **ETH** configurada com o endereço IP **192.168.1.20** e rodando uma aplicação Servidor OPC UA no CODESYS, com as variáveis iVar (INT) e iCount (INT) exportadas.



#### NOTA!

Qualquer PLC da WEG com CODESYS pode ser utilizado como **Servidor OPC UA**, desde que esteja previamente configurado, conforme detalhado na Seção 4 SERVIDOR OPC UA - CODESYS na página 4-1.

A Figura 8.2 na página 8-3 mostra a declaração de variáveis e a Figura 8.2 na página 8-3 apresenta o programa CODESYS em texto estruturado para a aplicação OPCUA\_PingPong.



Figura 8.2: Declaração de variáveis OPCUA\_PingPong.

Figura 8.3: Programa OPCUA\_PingPong em texto estruturado.

IF iVar = 0 THEN iVar := 1; iCount := iCount + 1; END\_IF

**OPCUA\_PingPong - Structured Text (ST)** 

IF iCount > 1000 THEN iCount := 0; END\_IF

#### 8.3.2 Cliente OPC UA - PLC500ED

o PLC500ED deve estar com a **ETH1** configurada com o endereço IP **192.168.1.10**, conectado à internet através da **ETH2**, executando o container **Edge Agent** e com uma aplicação WEGnology devidamente configurada. Nenhuma aplicação do CODESYS é necessária.

Na página principal da plataforma WEGnology, vá em **Workflows**  $\rightarrow$  **Edge Workflows**  $\rightarrow$  **Add**. Crie o *workflow* mostrado na Figura 8.4 na página 8-3, composto pelos blocos **Timer**, **OPC UA: Read**, **Conditional** e **OPC UA: Write**.



Figura 8.4: Workflow Cliente OPC UA.

Segue abaixo a descrição dos blocos e as respectivas configurações utilizadas:

**Timer**: define a periodicidade da execução do fluxo. Utilizado: 5 segundos.

OPC UA: Read: realiza a leitura de variáveis no Servidor OPC UA. São utilizadas as seguintes configurações:

- 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**: avalia uma condição lógica baseada nos valores lidos. Condição utilizada: {{iVar}} === '1'. **OPC UA: Write**: executa a escrita de variáveis no Servidor OPC UA. São utilizadas as seguintes configurações:

- 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!

Caso seja necessário confirmar o **Namespace Index** ou o **Identifier** das variáveis, pode ser útil utilizar o **UAExpert**. No **UAExpert**, ao acessar o Servidor OPC UA, é possível visualizar o **NodeID**, que exibe essas variáveis no formato: ns=4;s=|var|PLC410 Industrial.Application.OPCUA\_PingPong.

Ao finalizar o *workflow*, vá até o canto superior direito da tela, clique em **Deploy**, selecione o dispositivo e instale a aplicação em **Deploy Version**.



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