TECHDOCS

Technische Information

WAGO I/O System 750

750-8xxx

OPC-UA-Server

Version 1.1.0, FW-Version 03.06.09(18), OPC-UA-Server-Version 1.2.5

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Tel.: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technischer Support

Tel.: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich Fehler, trotz aller Sorgfalt, nie vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: documentation@wago.com

Inhaltsverzeichnis

1 Hinweise zu dieser Dokumentation 5
1.1 Gültigkeitsbereich 5
1.2 Urheberschutz 5
1.3 Schutzrechte 6
1.4 Symbole 7
1.5 Darstellung der Zahlensysteme 8
1.6 Schriftkonventionen 8
2 Wichtige Erläuterungen 9
2.1 Rechtliche Grundlagen 9
2.1.1 Änderungsvorbehalt 9
2.1.2 Personalqualifikation 9
2.1.3 Bestimmungsgemäße Verwendung der Serie 750 9
2.1.4 Technischer Zustand der Geräte 10
2.2 Sicherheitshinweise 11
2.3 Spezielle Einsatzbestimmungen für ETHERNET-Geräte 13
3 Überblick 14
4 Eigenschaften 15
4.1 Technische Daten 15
4.2 Versionskennungen für den OPC-UA-Server 16
4.3 Unterschiede zwischen dem WAGO OPC-UA-Server und dem 3S OPC-UA-Server 17
5 Funktionen 18
5.1 Netzwerk 18
5.1.1 Netzwerksicherheit 18
5.1.1.1 Authentifizierung 18
5.1.1.2 Autorisierung 18
5.1.1.3 Zertifikate 18
5.2 Einfluss von Variablentypen und ihre Auswirkungen auf Ausführungszeit und Laufzeit 19
5.2.1 Listenanfragen 19
5.2.2 Array-Anfragen 19
5.2.3 Strukturanfragen 19
5.2.4 Auswirkung der Datentypen der Runtime auf OPC-UA-Nodes 19
6 In Betrieb nehmen 21
6.1 Eine erste Verbindung zum OPC-UA-Server herstellen 21
6.1.1 Ungesicherte Verbindung herstellen 21
6.1.2 Gesicherte Verbindung herstellen und konfigurieren 25
6.2 Konfigurieren 27
6.2.1 Web-Based-Management (WBM) 27
6.2.1.1 Registerkarte „Fieldbus“ 28
6.2.1.1.1 Seite „OPC UA Status“ 28
6.2.1.1.2 Seite „OPC UA Configuration“ 29
6.2.1.1.3 Seite „OPC UA Information Model“ 32
7 Service 33

7.1 Neue Zertifikate installieren 33
7.2 OPC-UA-Clients hinzufügen 39

Abbildungsverzeichnis 42

Tabellenverzeichnis 43

1 Hinweise zu dieser Dokumentation

Hinweis

Dokumentation aufbewahren!
Diese Dokumentation ist Teil des Produkts. Bewahren Sie deshalb die Dokumentation während der gesamten Nutzungsdauer des Produkts auf. Geben Sie die Dokumentation an jeden nachfolgenden Benutzer des Produkts weiter. Stellen Sie darüber hinaus sicher, dass gegebenenfalls jede erhaltene Ergänzung in die Dokumentation mit aufgenommen wird.

1.1 Gültigkeitsbereich

Die vorliegende Dokumentation gilt für die Funktionalität „OPC-UA-Server“ in Zusammenhang mit der Software ***e!****COCKPIT* und einem WAGO Controller der PFC100- oder PFC200-Serie.

Die vorliegende Dokumentation gilt ab FW-Version 03.06.09(18), OPC-UA-Server-Version 1.2.5.

Die vorliegende, geräteübergreifende Dokumentation umfasst Funktionen und Eigenschaften, die nicht auf allen Geräten vorhanden sind.

Hinweis

Mitgeltende Dokumentationen beachten!
Beachten Sie neben dieser Dokumentation die Anweisungen und Informationen in den Betriebsanleitungen der eingesetzten Software und Geräte. Die Betriebsanleitung für die Software ***e!****COCKPIT* und für den verwendeten Controller (PFC100/PFC200) finden Sie auf der Internetseite http://www.wago.com im Downloadbereich.

1.2 Urheberschutz

1.3 Schutzrechte

In dieser Dokumentation werden Marken Dritter verwendet. Die verwendeten Marken entnehmen Sie diesem Kapitel. Im Weiteren wird auf das Mitführen der Zeichen „®“ und „™“ verzichtet.

- Adobe® und Acrobat® sind eingetragene Marken der Adobe Systems Inc.
- AS-Interface® ist eine eingetragene Marke der AS-International Association.
- BACnet® ist eine eingetragene Marke der American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® ist ein registriertes Warenzeichen der Bluetooth SIG, Inc.
- CiA® und CANopen® sind eingetragene Marken des CAN in AUTOMATION – International Users and Manufacturers Group e. V.
- DALI ist eine eingetragene Marke der Digital Illumination Interface Alliance (DiiA).
- EtherCAT® ist eine eingetragene Marke und eine patentierte Technologie der Beckhoff Automation GmbH.
- EtherNet/IP™ ist eine eingetragene Marke der Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® ist eine eingetragene Marke der EnOcean GmbH.
- IO-Link ist eine eingetragene Marke der PROFIBUS Nutzerorganisation e.V.
- KNX® ist eine eingetragene Marke der KNX Association cvba.
- Linux® ist eine eingetragene Marke von Linus Torvalds.
- LON® ist eine eingetragene Marke der Echelon Corporation.
- Modbus® ist eine registrierte Marke der Schneider Electric, lizenziert für die Modbus Organization, Inc.
- PROFIBUS® ist eine registrierte Marke der Siemens AG.
- PROFINET® ist eine registrierte Marke der Siemens AG.
- Subversion® ist eine Marke der Apache Software Foundation.
- Windows® ist eine registrierte Marke der Microsoft Corporation.

1.4 Symbole

GEFAHR

Warnung vor Personenschäden!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

GEFAHR

Warnung vor Personenschäden durch elektrischen Strom!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

WARNUNG

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit mittlerem Risiko, die Tod oder (schwere) Körperverletzung zur Folge haben kann, wenn sie nicht vermieden wird.

VORSICHT

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit geringem Risiko, die leichte oder mittlere Körperverletzung zur Folge haben könnte, wenn sie nicht vermieden wird.

ACHTUNG

Warnung vor Sachschäden!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

ESD

Warnung vor Sachschäden durch elektrostatische Aufladung!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

Hinweis

Wichtiger Hinweis!
Kennzeichnet eine mögliche Fehlfunktion, die aber keinen Sachschaden zur Folge hat, wenn sie nicht vermieden wird.

Information

Weitere Information
Weist auf weitere Informationen hin, die kein wesentlicher Bestandteil dieser Dokumentation sind (z. B. Internet).

1.5 Darstellung der Zahlensysteme

Tabelle 1: Darstellungen der Zahlensysteme

Zahlensystem	Beispiel	Bemerkung
Dezimal	100	Normale Schreibweise
Hexadezimal	0x64	C-Notation
Binär	'100' '0110.0100'	In Hochkomma, Nibble durch Punkt getrennt

1.6 Schriftkonventionen

Tabelle 2: Schriftkonventionen

Schriftart	Bedeutung
kursiv	Namen von Pfaden und Dateien werden kursiv dargestellt z. B.: *C:\Programme\WAGO Software*
Menü	Menüpunkte werden fett dargestellt z. B.: **Speichern**
>	Ein „Größer als“- Zeichen zwischen zwei Namen bedeutet die Auswahl eines Menüpunktes aus einem Menü z. B.: **Datei > Neu**
Eingabe	Bezeichnungen von Eingabe- oder Auswahlfeldern werden fett dargestellt z. B.: **Messbereichsanfang**
„Wert“	Eingabe- oder Auswahlwerte werden in Anführungszeichen dargestellt z. B.: Geben Sie unter **Messbereichsanfang** den Wert „4 mA“ ein.
[Button]	Schaltflächenbeschriftungen in Dialogen werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[Eingabe]**
[Taste]	Tastenbeschriftungen auf der Tastatur werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[F5]**

2 Wichtige Erläuterungen

Dieses Kapitel beinhaltet ausschließlich eine Zusammenfassung der wichtigsten Sicherheitsbestimmungen und Hinweise. Diese werden in den einzelnen Kapiteln wieder aufgenommen. Zum Schutz vor Personenschäden und zur Vorbeugung von Sachschäden an Geräten ist es notwendig, die Sicherheitsrichtlinien sorgfältig zu lesen und einzuhalten.

2.1 Rechtliche Grundlagen

2.1.1 Änderungsvorbehalt

Die WAGO Kontakttechnik GmbH & Co. KG behält sich Änderungen vor. Alle Rechte für den Fall der Patenterteilung oder des Gebrauchsmusterschutzes sind der WAGO Kontakttechnik GmbH & Co. KG vorbehalten. Fremdprodukte werden stets ohne Vermerk auf Patentrechte genannt. Die Existenz solcher Rechte ist daher nicht auszuschließen.

2.1.2 Personalqualifikation

Sämtliche Arbeitsschritte, die an den Geräten des WAGO I/O Systems 750 durchgeführt werden, dürfen nur von Elektrofachkräften mit ausreichenden Kenntnissen im Bereich der Automatisierungstechnik vorgenommen werden. Diese müssen mit den aktuellen Normen und Richtlinien für die Geräte und das Automatisierungsumfeld vertraut sein.

Alle Eingriffe in die Steuerung sind stets von Fachkräften mit ausreichenden Kenntnissen in der SPS-Programmierung durchzuführen.

2.1.3 Bestimmungsgemäße Verwendung der Serie 750

Feldbuskoppler, Controller und I/O-Module des modularen WAGO I/O Systems 750 dienen dazu, digitale und analoge Signale von Sensoren aufzunehmen und an Aktoren auszugeben oder an übergeordnete Steuerungen weiterzuleiten. Mit den Controllern ist zudem eine (Vor-)Verarbeitung möglich.

Die Geräte sind für ein Arbeitsumfeld entwickelt, welches der Schutzart IP20 genügt und für den Einsatz in trockenen Innenräumen ausgelegt.
Es besteht Fingerschutz und Schutz gegen feste Fremdkörper ≥ 12,5 mm, jedoch kein Schutz gegen Wasser. Der Betrieb der Geräte in nasser und staubiger Umgebung ist nicht gestattet, sofern nicht anders angegeben.
Ein Einsatz ohne Schutzmaßnahmen in einer Umgebung, in der Feuchtigkeit, Staub, ätzende Dämpfe, Gase oder ionisierende Strahlung auftreten können, gilt als sachwidrige Verwendung.

Der Betrieb von Geräten des WAGO I/O Systems 750 im Wohnbereich ist ohne weitere Maßnahmen nur zulässig, wenn diese die Emissionsgrenzen (Störaussendungen) gemäß EN 61000-6-3 einhalten. Entsprechende Angaben

finden Sie im Kapitel „Gerätebeschreibung“ > „Normen und Richtlinien“ im Handbuch zum eingesetzten Gerät.

Für den Betrieb des WAGO I/O Systems 750 in explosionsgefährdeten Bereichen ist ein entsprechender Gehäuseschutz gemäß der Richtlinie 2014/34/EU erforderlich. Beachten Sie die Errichtungsbestimmungen! Zusätzlich ist zu beachten, dass eine Baumusterprüfbescheinigung erwirkt werden muss, die den korrekten Einbau des Systems im Gehäuse bzw. Schaltschrank bestätigt.

Die Realisierung von Sicherheitsfunktionen wie NOT-HALT-Einrichtungen oder Schutztürüberwachungen darf nur von den F-I/O-Modulen des modularen WAGO I/O Systems 750 ausgeführt werden. Nur diese sicheren F-I/O-Module gewährleisten funktionale Sicherheit gemäß den aktuellen internationalen Normen. Rückwirkungsfreie Ausgangsmodule von WAGO können von der Sicherheitsfunktion angesteuert werden.

2.1.4 Technischer Zustand der Geräte

Die Geräte werden ab Werk für den jeweiligen Anwendungsfall mit einer festen Hard- und Softwarekonfiguration ausgeliefert. Sie enthalten keine durch den Anwender zu wartenden oder zu reparierenden Teile. Folgende Handlungen bewirken den Haftungsausschluss der WAGO Kontakttechnik GmbH & Co. KG:

- Reparaturen,
- Veränderungen an der Hard- oder Software, die nicht in der Bedienungsanleitung beschrieben sind,
- nicht bestimmungsgemäßer Gebrauch der Komponenten.

Weitere Einzelheiten ergeben sich aus den vertraglichen Vereinbarungen. Wünsche an eine abgewandelte bzw. neue Hard- oder Softwarekonfiguration richten Sie bitte an die WAGO Kontakttechnik GmbH & Co. KG.

2.2 Sicherheitshinweise

Beim Einbauen des Gerätes in Ihre Anlage und während des Betriebes sind folgende Sicherheitshinweise zu beachten:

GEFAHR

Nicht an Geräten unter Spannung arbeiten!
Schalten Sie immer alle verwendeten Spannungsversorgungen für das Gerät ab, bevor Sie es montieren, Störungen beheben oder Wartungsarbeiten vornehmen.

GEFAHR

Produkt nur in einem geeigneten Gehäuse einbauen!
Das Produkt ist ein offenes Betriebsmittel. Montieren Sie das Produkt in einem geeigneten Gehäuse. Dieses Gehäuse muss:

- gewährleisten, dass der max. zulässige Verschmutzungsgrad nicht überschritten wird.
- einen ausreichenden Schutz gegen Berühren bieten.
- einen ausreichenden Schutz gegen UV-Einstrahlung bieten.
- die Ausbreitung von Feuer nach außerhalb des Gehäuses verhindern.
- die Festigkeit gegen mechanische Beanspruchung gewährleisten.
- den Zugang auf autorisiertes Fachpersonal einschränken und darf nur mit Werkzeug zu öffnen sein.

GEFAHR

Trennvorrichtung und Überstromschutz gewährleisten!
Das Gerät ist für den Einbau in Anlagen der Automatisierungstechnik vorgesehen. Es verfügt nicht über eine integrierte Trennvorrichtung. Angeschlossene Anlagen müssen abgesichert werden.
Sehen Sie anlagenseitig eine geeignete Trennvorrichtung und einen geeigneten Überstromschutz vor.

GEFAHR

Unfallverhütungsvorschriften beachten!
Beachten Sie bei Montage, Inbetriebnahme, Betrieb, Wartung und Störbehebung die für Ihre Maschine/Anlage zutreffenden Unfallverhütungs-vorschriften wie beispielsweise die DGUV Vorschrift 3 „Elektrische Anlagen und Betriebsmittel“.

GEFAHR

Auf normgerechten Anschluss achten!
Zur Vermeidung von Gefahren für das Personal und Störungen an Ihrer Anlage, verlegen Sie die Daten- und Versorgungsleitungen normgerecht und achten Sie auf die korrekte Anschlussbelegung. Beachten Sie die für Ihre Anwendung zutreffenden EMV-Richtlinien.

ACHTUNG

Nicht in Telekommunikationsnetzen einsetzen!
Verwenden Sie Geräte mit ETHERNET-/RJ-45-Anschluss ausschließlich in LANs. Verbinden Sie diese Geräte niemals mit Telekommunikationsnetzen, wie z. B. mit Analog- oder ISDN-Telefonanlagen.

ACHTUNG

Einwandfreie Kontaktierung zur Tragschiene gewährleisten!
Der einwandfreie, elektrische Kontakt zwischen Tragschiene und Gerät ist notwendig, um die EMV-Eigenschaften und Funktion des Gerätes aufrechtzuerhalten.

ACHTUNG

Defekte oder beschädigte Geräte austauschen!
Tauschen Sie defekte oder beschädigte Geräte (z. B. bei deformierten Kontakten) aus.

ACHTUNG

Geräte vor kriechenden und isolierenden Stoffen schützen!
Die Geräte sind unbeständig gegen Stoffe, die kriechende und isolierende Eigenschaften besitzen, z. B. Aerosole, Silikone, Triglyceride (Bestandteil einiger Handcremes). Sollten Sie nicht ausschließen können, dass diese Stoffe im Umfeld der Geräte auftreten, bauen Sie die Geräte in ein Gehäuse ein, das resistent gegen oben genannte Stoffe ist. Verwenden Sie generell zur Handhabung der Geräte saubere Werkzeuge und Materialien.

ACHTUNG

Nur mit zulässigen Materialien reinigen!
Reinigen Sie das Gehäuse und verschmutzte Kontakte mit Propanol.

ACHTUNG

Kein Kontaktspray verwenden!
Verwenden Sie kein Kontaktspray, da in Verbindung mit Verunreinigungen die Funktion der Kontaktstelle beeinträchtigt werden kann.

ACHTUNG

Verpolungen vermeiden!
Vermeiden Sie die Verpolung der Daten- und Versorgungsleitungen, da dies zu Schäden an den Geräten führen kann.

ESD

Elektrostatische Entladung vermeiden!
In den Geräten sind elektronische Komponenten integriert, die Sie durch elektrostatische Entladung bei Berührung zerstören können. Beachten Sie die Sicherheitsmaßnahmen gegen elektrostatische Entladung gemäß DIN EN 61340-5-1/-3. Achten Sie beim Umgang mit den Geräten auf gute Erdung der Umgebung (Personen, Arbeitsplatz und Verpackung).

2.3 Spezielle Einsatzbestimmungen für ETHERNET-Geräte

Wo nicht speziell beschrieben, sind ETHERNET-Geräte für den Einsatz in lokalen Netzwerken bestimmt. Beachten Sie folgende Hinweise, wenn Sie ETHERNET-Geräte in Ihrer Anlage einsetzen:

- Verbinden Sie Steuerungskomponenten und Steuerungsnetzwerke nicht direkt mit einem offenen Netzwerk wie dem Internet oder einem Büronetzwerk. WAGO empfiehlt, Steuerungskomponenten und Steuerungsnetzwerke hinter einer Firewall anzubringen.

- Schließen Sie alle nicht von Ihrer Applikation benötigten Ports und Dienste in den Steuerungskomponenten (z. B. für WAGO-I/O-CHECK und CODESYS), um die Gefahr von Cyber-Angriffen zu verringern und damit die Cyber-Security zu erhöhen.
  Öffnen Sie die Ports und Dienste nur für die Dauer der Inbetriebnahme bzw. Konfiguration.

- Beschränken Sie den physikalischen und elektronischen Zugang zu sämtlichen Automatisierungskomponenten auf einen autorisierten Personenkreis.

- Ändern Sie vor der ersten Inbetriebnahme unbedingt die standardmäßig eingestellten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.

- Ändern Sie regelmäßig die verwendeten Passwörter! Sie verringern so das Risiko, dass Unbefugte Zugriff auf Ihr System erhalten.

- Ist ein Fernzugriff auf Steuerungskomponenten und Steuerungsnetzwerke erforderlich, sollte ein „Virtual Private Network“ (VPN) genutzt werden.

- Führen Sie regelmäßig eine Bedrohungsanalyse durch. So können Sie prüfen, ob die getroffenen Maßnahmen Ihrem Schutzbedürfnis entsprechen.

- Wenden Sie in der sicherheitsgerichteten Gestaltung Ihrer Anlage „Defense-in-depth“-Mechanismen an, um den Zugriff und die Kontrolle auf individuelle Produkte und Netzwerke einzuschränken.

3 Überblick

OPC Unified Architecture ist eine Plattform-unabhängige und Service-orientierte Architektur. Sie wird verwendet, um Daten zu beschreiben und zu transportieren. Durch die Unabhängigkeit der Services können Geräte verschiedener Anbieter miteinander verbunden werden.
Der beschriebene Server kann Daten der Runtime der PFC100 und PFC200 Serie veröffentlichen, wenn das verwendete Produkt die benötigten Voraussetzungen besitzt. Das Gerät muss eine ETHERNET-Schnittstelle haben, die für die Kommunikation verwendet werden kann. Das Gerät muss den vom Server benötigten Speicher sowie die benötigte Prozessorzeit bereitstellen.

4 Eigenschaften

4.1 Technische Daten

- Der OPC-UA-Server unterstützt die Variablen der ***e!****Runtime*-Laufzeitumgebung. Die zu überwachenden Variablen müssen über die Symbolkonfiguration freigegeben werden.
- Der Server unterstützt 1000 „Monitored Items“ pro Subscription.
- Folgende Datentypen sind möglich:
  `BOOL, BYTE, WORD, DWORD, LWORD, SINT, INT, DINT, LINT, USINT, UINT, UDINT, ULINT, REAL, LREAL, TIME, LTIME, TIME_OF_DAY, DATE, DATE_AND_TIME, STRING, WSTRING, ENUM, ARRAY, STRUCT`

Hinweis

Einschränkungen für Strukturen und Arrays
Strukturen, die Enumerationen enthalten, werden nicht unterstützt. Arrays, die einen Enumerations-Datentyp enthalten, werden nicht unterstützt.

- Der Server unterstützt benutzerdefinierte IEC-Datentypen (Strukturen und Enumerationen).
- Der Server kann ohne Laufzeitsystem betrieben werden. Er ist in seinen Rechten im System begrenzt (Sicherheit).
- Der Server läuft unabhängig vom Laufzeitsystem und kann somit separat gestartet und gestoppt werden.
- Der Server unterstützt verschlüsselte Kommunikation.
- Ein Login ist anonym oder mit Benutzername/Passwort möglich.
- Der Server kann mit vertrauenswürdigen Zertifikaten betrieben werden.
- Der Server kann mit bis zu 7 Clients parallel betrieben werden.
- Der Server kann Client-Zertifikate verwalten. (Anfragen von unbekannten Clients werden abgewiesen.)

Hinweis

Anzahl der OPC-UA-Knoten abhängig von Systemleistung
Die Anzahl der OPC-UA-Knoten, die der OPC-UA-Server zur Verfügung stellen kann, ist abhängig von der verfügbaren Systemleistung. Daher kann hier keine pauschale Aussage getroffen werden.
Sowohl die IEC-Applikation als auch sonstige Systemfunktionen beeinflussen diese Anzahl. So kann z. B. eine ressourcenschonende Programmierung des Gerätes die mögliche Anzahl der OPC-UA-Knoten deutlich steigern.

4.2 Versionskennungen für den OPC-UA-Server

Der Server besteht aus verschiedenen Teilen. Jeder Teil besitzt eine eigene Versionskennung. Die Teile sind in der nachfolgenden Tabelle aufgelistet.

Tabelle 3: Teile des OPC-UA-Servers

Teil des OPC-UA-Servers	Versionsabfrage
WAGO OPC-UA-Server	Die Version kann über das Server-Executable erfragt werden (/usr/bin/opcua-server -v).
Im Server verwendete SDK-Version	Die Version kann über das Server-Executable erfragt werden (/usr/bin/opcua-server -s).
WAGO OPC-UA-Konfigtool	Die Version kann über das Konfigtool erfragt werden (/etc/config-tool/config-opcua -v).

Alle Versionen können über eine ssh-Shell angefordert werden. Im WBM wird die Version des WAGO OPC-UA-Servers angezeigt. Diese Version impliziert eine bestimmte SDK-Version.

Das Konfigtool ist für den Betrieb des Servers nicht relevant. Mit den Build-Informationen, die über das OPC-UA-Protokoll veröffentlicht werden, wird die WAGO OPC-UA-Server-Version veröffentlicht.

4.3 Unterschiede zwischen dem WAGO OPC-UA-Server und dem 3S OPC-UA-Server

Der WAGO OPC-UA-Server weicht in folgenden Punkten vom 3S OPC-UA-Server ab:

- Der Variablenparameter “MinimumSamplingInterval” ist für keine Variable auslesbar.
- Die PLC Open Datentypen BYTE, WORD, DWORD, LWORD, DT, TOD sind nicht vorhanden.
  IEC-Variablen mit diesen Datentypen werden auf OPC-Standarddatentypen mit der gleichen Größe abgebildet.
- Die Daten des Laufzeitsystems sind im Verzeichnis „DeviceSet“ abgelegt. Es wird kein weiteres Mapping der Daten unter dem Verzeichnis „Server“ angeboten.
- Enumerationen (Enum) verwenden einen ReferenceType aus dem Verzeichnis „BaseDataVariableType“. Dieser ReferenceType wurde durch den original installierten Server im Verzeichnis „BaseVariableType“ angelegt.
- Der 3S OPC-UA-Server verwendet standardmäßig einen anderen Namespace als der WAGO OPC-UA-Server.

5 Funktionen

5.1 Netzwerk

5.1.1 Netzwerksicherheit

5.1.1.1 Authentifizierung

Der OPC-UA-Server nutzt unter Linux die im System definierten Benutzer, die eine Login-Möglichkeit besitzen. Im Auslieferungszustand sind das die Folgenden:

- root
- admin
- user

5.1.1.2 Autorisierung

Ein Autorisierungskonzept besteht derzeit nicht. Somit sind zurzeit keine Einschränkungen für den „anonymus“-Benutzer zu erwarten, wenn sein Zugriff über die Konfiguration eingeschränkt wird.

5.1.1.3 Zertifikate

Der Server ist im Auslieferungszustand mit einem Zertifikat ausgestattet. Dieses ausgelieferte Zertifikat besitzt jedoch eine geringe Sicherheit.

Daher ist es sinnvoll, das vorhandene Zertifikat gegen ein geeignetes Zertifikat auszutauschen, welches einem höherem Sicherheitsstandard genügt.

Für den Zertifikatstausch kann die GDS-Push Methode angewendet werden.

Der Zertifikatstausch mit UA-Expert ist im Kapitel „Service“ > „Neue Zertifikate installieren“ näher beschrieben.

5.2 Einfluss von Variablentypen und ihre Auswirkungen auf Ausführungszeit und Laufzeit

Das Verhältnis von Protokolldaten zu Nutzdaten beeinflusst den Datendurchsatz. Die Nutzdatenmenge eines OPC-UA-Nodes ist in der Regel fest. Wenn zum Beispiel ein OPC-UA-Node mit dem Datentyp „Byte“ verwendet wird, dann ist die Nutzdatenmenge bei der Anfrage dieses Nodes 1 Byte. Um die Nutzdatenmenge zu erhöhen, können drei Verfahren verwendet werden:

- Zusammenfassen von mehreren Nodes in einer Anfrage (Listen).
- Zusammenfassen von gleichen Datentypen unter einem Node (Arrays).
- Zusammenfassen von ungleichen Datentypen unter einem Node (Strukturen).

5.2.1 Listenanfragen

Wenn OPC-UA-Nodes zu einer Liste zusammengefügt werden, so werden die Informationen jedes einzelnen Nodes bei der Anfrageaktion transportiert und ausgewertet. Das Verhältnis Nutzdatenmenge zu Nodes ist gleich, das Verhältnis Nutzdatenmenge zu Anfragen verbessert sich.

5.2.2 Array-Anfragen

Wenn Arrays als OPC-UA-Nodes verwendet werden, so wächst die Nutzdatenmenge mit der Größe des verwendeten Arrays. Die Einzelelemente sind immer gleich groß. Die logische Benennung ist auf den Knotennamen begrenzt.

5.2.3 Strukturanfragen

Wenn Strukturen als OPC-UA-Nodes verwendet werden, so wächst die Nutzdatenmenge mit der Größe der verwendeten Struktur. Um Werte von Strukturvariablen, welche für die Übertragung enkodiert wurden, im Client zu interpretieren, werden weitere Informationen benötigt. Diese Informationen sind im „Data Type Dictionary“ des Servers abgelegt, und können vom Client separat angefordert werden. Somit können die Information zum Decodieren einmal angefordert werden, und dann bei Eintreffen von neuen Daten wiederverwendet werden.

5.2.4 Auswirkung der Datentypen der Runtime auf OPC-UA-Nodes

Die Datentypen von Variablen der Runtime sind analog zu den Datentypen, die der OPC-UA-Server anbietet. Hierdurch ergibt sich, dass die Auswahl der Datentypen in der Runtime einen wichtigen Einfluss auf die Verarbeitungslast (benötigte CPU-Last) der veröffentlichten OPC-UA-Daten hat.

Beispielsweise erzeugen 10 Einzelvariablen (über OPC-UA veröffentlicht) eine höhere Verarbeitungslast als eine Strukturvariable mit 10 Feldern.

6 In Betrieb nehmen

6.1 Eine erste Verbindung zum OPC-UA-Server herstellen

6.1.1 Ungesicherte Verbindung herstellen

Um eine Verbindung mit einem OPC-UA-Server herzustellen, wird ein OPC-UA-Client benötigt. Die nachfolgende Beschreibung bezieht sich auf den Client „UAExpert“ der Firma „Unified Automation GmbH“.

Der WAGO OPC-UA-Server besitzt für die Erstinbetriebnahme einen speziellen Inbetriebnahmemodus. Dieser ist solange aktiv, wie noch keine vertrauenswürdigen Zertifikate auf dem Server vorhanden sind.

Hinweis

Datum und Uhrzeit von Server und Client abgleichen!
Für eine (durch Zertifikate abgesicherte) Verbindung zwischen Client und Server müssen das Datum und die Uhrzeit von Client und Server abgeglichen sein.
Aktualisieren Sie ggf. das Datum und die Uhrzeit auf dem Controller.

PC mit OPC-UA-Client

1. Starten Sie „UAExpert“.
2. Erstellen Sie ein neues Projekt.
3. Klicken Sie die Schaltfläche **[+]** in der Menüleiste des Clients, um einen Server hinzuzufügen.

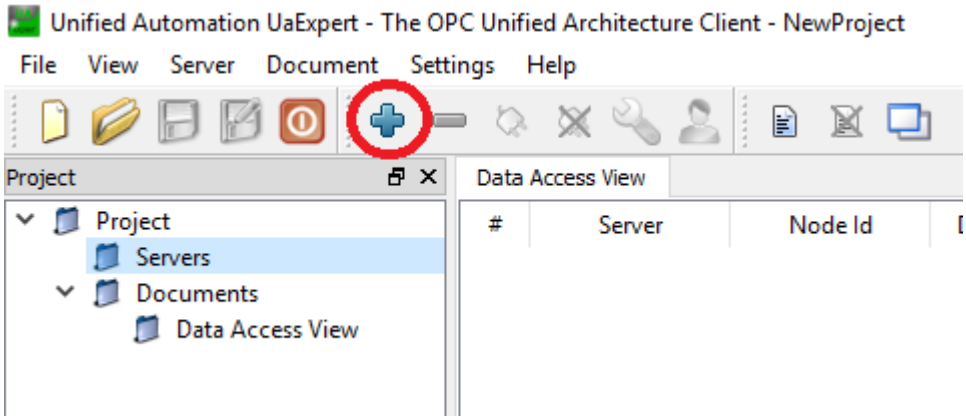

Abbildung 1: Oberfläche des UAExpert

4. Öffnen Sie mit einem Doppelklick auf den Eintrag „**+ <Double Click to Add Server>**“ das Eingabefenster für die URL des Servers.

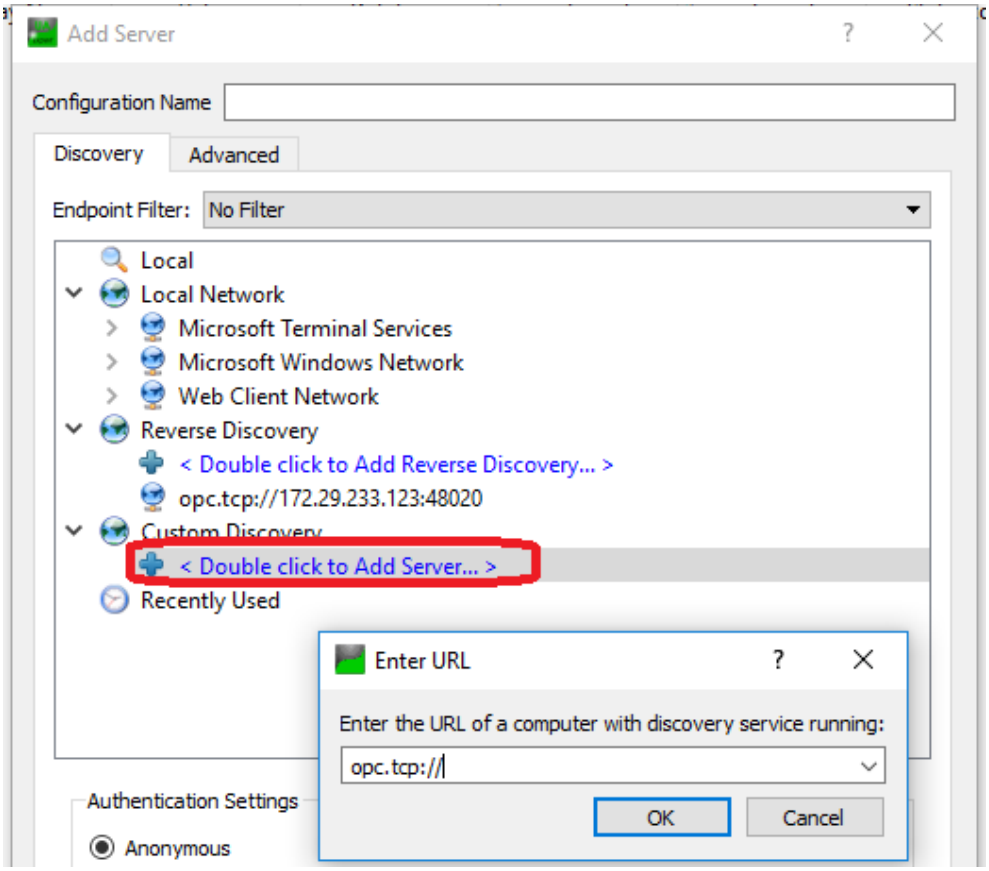

Abbildung 2: Hinzufügen eines Servers

5. Geben sie für die URL „opc.tcp://[Domainname oder IP-Adresse]“ ein.
6. Bestätigen Sie die Eingabe mit **[OK]**.
7. Wählen Sie die soeben eingegebene URL aus.
8. Wählen Sie unter der URL den OPC-UA-Server aus.
9. Bestätigen Sie die Abfrage im Meldungsfenster.
10. Wählen Sie die gesicherte Verbindung („Basic256Sha256“) aus.
11. Wählen Sie im Bereich „**Authentication Settings**“ die Option „**Username/Password**“ aus.
12. Geben Sie den Usernamen (im Auslieferungszustand „root“) ein.
13. Markieren Sie das Kontrollfeld „**Store**“.
14. Geben Sie das Passwort (im Auslieferungszustand „wago“) ein.
15. Klicken Sie **[OK]**, um die Eingaben zu übernehmen.

Alternativ können Sie den Usernamen und das Passwort auch wie nachfolgend beschrieben über den Eigenschaftendialog des Servers anlegen oder ändern.

16. Öffnen Sie im Projektbaum unter „**Project**“ > „**Servers**“ das Kontextmenü des soeben angelegten Servers mit der rechten Maustaste.

17. Wählen Sie den Menüpunkt „**Properties**“ aus.

18. Geben Sie wie oben beschrieben den Usernamen und das Passwort ein.

19. Bestätigen Sie die Eingaben mit **[OK]**.

→ Die Verbindungsparameter sind nun angelegt.

20. Öffnen Sie in der Baumstruktur unter „**Servers**“ das Kontextmenü des soeben angelegten Servers aus und wählen Sie den Menüpunkt „**Connect**“.

Bei der ersten Verbindung mit dem Server muss das mit dem Server ausgelieferte Zertifikat in die Liste der glaubwürdigen Zertifikate des Clients übernommen werden.

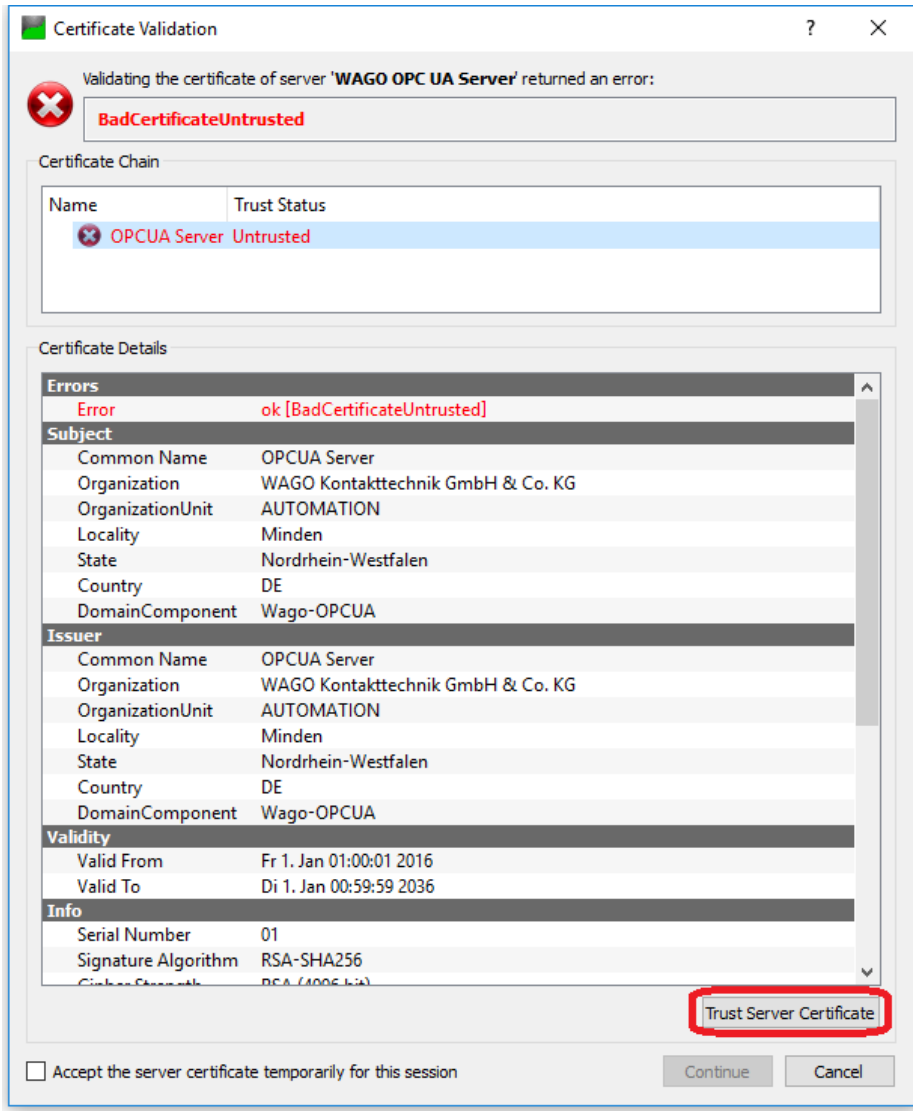

Abbildung 3: Bestätigung des Server-Zertifikats

21. Klicken Sie im Fenster „**Certificate Validation**“ die Schaltfläche **[Trust Server Certificate]**., um das Zertifikat zu übernehmen.

22. Klicken Sie **[Continue]**, um das Fenster zu schließen und die Verbindung herzustellen.

Hinweis

Zertifikat austauschen!
Dieses Zertifikat wird mit allen Servern ausgeliefert und besitzt eine geringe Sicherheit.
Tauschen Sie das mitgelieferte Zertifikat gegen ein Zertifikat mit höherem Sicherheitsstandard aus.

Wenn eine verschlüsselte Verbindung aufgebaut wird, dann werden der Hostname sowie die Eintragungen im Zertifikat geprüft.
Wenn die Angaben nicht übereinstimmen, wird die nachfolgende Meldung angezeigt.

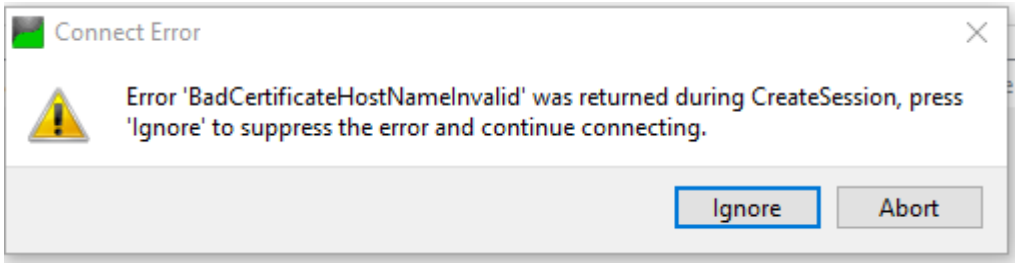

Abbildung 4: Meldung bei Verbindungsaufbau

23. Klicken Sie im Meldungsfenster die Schaltfläche **[Ignore]**, um die Verbindung trotzdem herzustellen.

→ Damit ist eine erste, ungesicherte Verbindung aufgebaut.

6.1.2 Gesicherte Verbindung herstellen und konfigurieren

Für eine gesicherte Verbindung muss noch das Zertifikat ausgetauscht werden. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie im Projektbaum unter „**Projects**“ das Kontextmenü des Eintrags „**Documents**“ das Kontextmenü mit der rechten Maustaste.

2. Wählen Sie den Menüpunkt „**Add …**“, um ein „GDS Push View“-Dokument hinzuzufügen.

3. Klicken Sie im nachfolgenden Fenster auf die Schaltfläche **[Add]**, um das Hinzufügen zu bestätigen.

4. Öffnen Sie das Register „**GDS Push View**“.

5. Klicken Sie im Bereich „**Server Certificate**“ auf die Schaltfläche **[Create Certificate …]**.

6. Klicken Sie auf die Schaltfläche **[OK]**, um den nachfolgenden Hinweis zu bestätigen.

7. Nehmen Sie die notwendigen Einstellungen vor.

8. Klicken Sie auf die Schaltfläche **[OK]**, um die Einstellungen zu bestätigen.

9. Klicken Sie auf die Schaltfläche **[Download]**, um das Zertifikat in den Controller zu laden.

→ Ein Meldungsfenster mit einer Abfrage wird geöffnet.

10. Klicken Sie auf die Schaltfläche **[No]**, um das Zertifikat unverändert zu übernehmen und das Meldungsfenster zu schließen.

→ Ein weiteres Meldungsfenster mit einer Erinnerung wird geöffnet.

11. Klicken Sie auf die Schaltfläche **[OK]**, um die Erinnerung zu quittieren und dieses Meldungsfenster zu schließen.

12. Klicken Sie auf die Schaltfläche **[Apply Changes]**, um den Vorgang abzuschließen.

13. Klicken Sie auf die Schaltfläche **[Disconnect]**, um die Verbindung zu trennen.

14. Klicken Sie auf die Schaltfläche **[Connect]**, um die Verbindung wiederherzustellen.

15. Klicken Sie im Fenster „**Certificate Validation**“ die Schaltfläche **[Trust Server Certificate]**., um das Zertifikat zu übernehmen.

Wenn eine verschlüsselte Verbindung aufgebaut wird, dann werden der Hostname sowie die Eintragungen im Zertifikat geprüft.
Wenn die Angaben nicht übereinstimmen, wird die nachfolgende Meldung angezeigt.

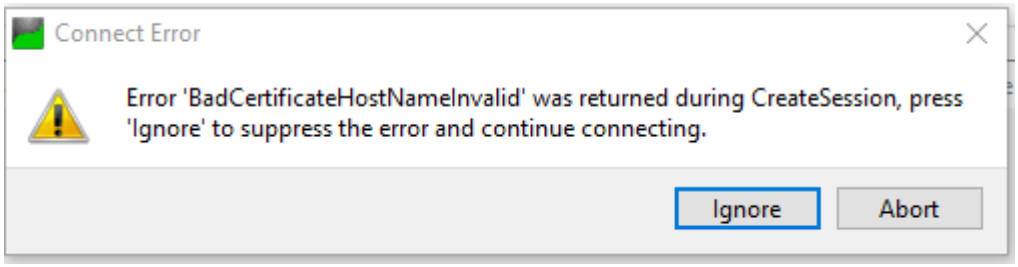

Abbildung 5: Meldung bei Verbindungsaufbau

16. Klicken Sie im Meldungsfenster die Schaltfläche **[Ignore]**, um die Verbindung trotzdem herzustellen.

→ Im Fenster „**GDS Push View**“ im Bereich „**Server Certificate Groups**“ finden Sie nun im Register **„Trusted“** ein noch nicht als vertrauenswürdig eingestuftes, von „UAExpert“ erstelltes Zertifikat. Dieses Zertifikat ist durch ein rotes „X“ gekennzeichnet.

17. Öffnen Sie das Kontextmenü dieses Zertifikatseintrags mit der rechten Maustaste.

18. Wählen Sie den Menüpunkt „**Trust**“.

→ Das Zertifikat wird nun auf dem Server ausgetauscht. Das ausgetauschte Zertifikat ist durch einen grünen Haken gekennzeichnet.

19. Speichern Sie die Einstellungen für eine spätere Verwendung in einem neuen Projekt.

→ Damit ist nur noch eine über ein entsprechendes Zertifikat abgesicherte Verbindung zum Server möglich. Der Inbetriebnahmemodus wird automatisch beendet. Andere Clients ohne entsprechendes Zertifikat können den Server somit nicht mehr erreichen.

6.2 Konfigurieren

Der WAGO OPC-UA-Server kann über das Web-Based-Management (WBM) konfiguriert werden.

6.2.1 Web-Based-Management (WBM)

Die Informationen und Einstellungen für den WAGO OPC-UA-Server sind auf den WBM-Seiten „**OPC UA Status**“, „**OPC UA Configuration**“ und „**OPC UA Information Model**“ dargestellt.

Die Seiten sind über das Register „**Fieldbus**“ und den Auswahlpunkt „**OPC UA**“ erreichbar.

6.2.1.1 Registerkarte „Fieldbus“

6.2.1.1.1 Seite „OPC UA Status“

Auf der Seite „OPC UA Status“ finden Sie Statusinformationen zum OPC-UA-Dienst.

Gruppe „OPC UA Server“

Tabelle 4: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server“

Parameter	Bedeutung
State	Hier wird der aktuelle Status (enabled/disabled) des WAGO OPC-UA-Servers angezeigt.
Version	Hier wird die installierte Version des WAGO OPC-UA-Servers angezeigt.
License	Hier wird eine ggf. vorhandenen OPC-UA-Server-Lizenz angezeigt. Einige Features des WAGO OPC-UA-Servers setzen eine spezielle kostenpflichtige Lizenz voraus.

6.2.1.1.2 Seite „OPC UA Configuration“

Auf der Seite „OPC UA Configuration“ finden Sie die Einstellungen zum OPC-UA-Dienst.

Gruppe „General OPC UA Server Configuration“

Tabelle 5: WBM-Seite „OPC UA Configuration“ – Gruppe „General OPC UA Server Configuration“

Parameter	Bedeutung	
Service enabled	Hier aktivieren oder deaktivieren Sie den WAGO OPC-UA-Server.	
Ctrl Configuration name	Hier geben Sie den Konfigurationsnamen an, den der Controller innerhalb des PLC Open Device Sets erhält.	
Log level	Hier wählen Sie den Log-Level aus. Folgende Werte sind einstellbar: Info / Debug / Warning / Error. Mit dem Log-Level „Error“ werden nur Fehlermeldungen ausgegeben, mit dem Log-Level „Info“ auch Statusmeldungen. Die Auswahl des Log-Levels beeinflusst die Reaktionszeit des Servers. Wählen Sie daher nur den minimal benötigten Level aus, z. B. „Debug“ nur für tiefgreifende Analysen.	
Unlimited anonymous access	Hier stellen Sie die Rechte für den Zugriff auf die vom Server bereitgestellten Daten ein.	
	Enabled	Ein nicht registrierter Benutzer kann alle Variablen sehen, lesen und schreiben.
	Disabled	Für den Vollzugriff auf die Daten ist ein Benutzer-Login mit den passenden Rechten erforderlich.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „OPC UA Endpoints“

Tabelle 6: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Endpoints“

Parameter	Bedeutung
Security Policy - None	Hier aktivieren oder deaktivieren Sie den OPC-UA-Endpoint „None“. Dieser ermöglicht, eine ungesicherte Verbindung zum OPC-UA-Server aufzubauen.
Security Policy - Basic128Rsa15	Hier aktivieren oder deaktivieren Sie die Security-Policy „Basic128Rsa15“. **Hinweis:** Diese Policy wird nicht mehr als sicher eingestuft.
Security Policy - Basic256Sha256	Die Security-Policy „Basic256Sha256“ ermöglicht, eine gesicherte Verbindung mit dem OPC-UA-Server aufzubauen.

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Gruppe „OPC UA Security Settings“

Tabelle 7: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Security Settings“

Parameter	Bedeutung	
Trust all clients	Hier aktivieren oder deaktivieren Sie die Verifikation.	
	Enabled	Es wird eine Verbindung zu allen Clients erlaubt. → Keine Sicherheit!
	Disabled	Es wird nur eine Verbindung zu Clients mit sichern Zertifikaten zugelassen.
Application URI Check	Hier aktivieren oder deaktivieren Sie die URI-Prüfung. Eine deaktivierte URI-Prüfung ermöglicht es, eine Verbindung zu einem OPC-Server aufzubauen, auch wenn dessen URI sich von der in den Zertifikaten hinterlegten URI unterscheidet.	
Error Certificate Time	Hier aktivieren oder deaktivieren Sie die Zeitüberprüfung. Zertifikate können ein Ablaufdatum besitzen. Dieses Datum wird mit der aktuellen Zeit des Gerätes überprüft. Wenn das Gerät eine falsch eingestellte Zeit besitzt, kann die Prüfung nicht erfolgreich durchgeführt werden.	
Certificate Issuer Time Invalid	Hier aktivieren oder deaktivieren Sie die Überprüfung des Zeitstempels. CA-Zertifikate enthalten einen Zeitstempel bzw. eine Gültigkeit vom Aussteller. Dieser wird mit Hilfe der Zeit auf der Server-Hardware überprüft. Durch eine fehlerhafte bzw. nicht vorhandene Zeiteinstellung auf der Server-Hardware kann es dazu kommen, dass das Zertifikat als ungültig gekennzeichnet wird.	
Certificate Revocation Unknown	Hier aktivieren oder deaktivieren Sie die Überprüfung der Erreichbarkeit des Speicherortes für zurückgezogene Zertifikate. Jedes Zertifikat kann einen Ort für zurückgezogene Zertifikate besitzen. Falls der angegebene Ort z. B. durch Netzwerkprobleme nicht erreicht werden kann, wird das Zertifikat nicht akzeptiert.	
Certificate Issuer Revocation Unknown	Hier aktivieren oder deaktivieren Sie die Überprüfung der Erreichbarkeit des Ablageortes für zurückgezogene Zertifikate. Jedes Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) kann eine Angabe für den Ablageort von zurückgezogenen Zertifikaten enthalten. Kann dieser Ort nicht erreicht werden, wird das Zertifikat vom Server nicht akzeptiert.	

Um die Änderungen zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

6.2.1.1.3 Seite „OPC UA Information Model“

Auf der Seite „OPC UA Information Model“ finden Sie die Einstellungen zum OPC-UA-Informationsmodell.
Die Seite ist nur sichtbar bei Controllern der 2. Generation (750-821x/xxx-xxx), die Softwarekomponenten unterstützen, die einer Lizenzprüfung unterliegen (Runtime-Lizenzen).

Gruppe „OPC UA Server Information Model“

Tabelle 8: WBM-Seite „OPC UA Information Model“ – Gruppe „OPC UA Server Information Model“

Parameter	Bedeutung
Feature enabled	Hier aktivieren oder deaktivieren Sie das OPC UA Server-Informationsmodell.
informationmodel.xml	Hier wählen Sie eine XML-Beschreibungsdatei für das anzuwendende Informationsmodell aus. Die Verwendung eines spezifischen Informationsmodells setzt eine erweiterte OPC UA Lizenz voraus!

Um eine Änderung zu übernehmen, klicken Sie die Schaltfläche **[Submit]**.

Um die ausgewählte Beschreibungsdatei auf den Controller zu übertragen, klicken Sie die Schaltfläche **[Upload]**.

Um die installierte Beschreibungsdatei vom Controller zu löschen, klicken Sie die Schaltfläche **[Delete]**. Nach dem Löschen wird wieder das standardmäßig installierte PLC-Open-Informationsmodell verwendet.

7 Service

7.1 Neue Zertifikate installieren

Um Änderungen an den Zertifikaten vornehmen zu können, wird eine verschlüsselte authentifizierte Verbindung benötigt.

Hinweis

Nur temporär alle Clients zulassen!
Wenn der Aufbau einer verschlüsselten Verbindung zum OPC-UA-Server nicht möglich ist, aktivieren Sie die Option **Trust all Clients** im WBM, damit der OPC-UA-Server eine Verbindung mit allen Clients akzeptiert. Deaktivieren sie die Option, nachdem Sie die nachfolgenden Schritte vollständig durchgeführt haben!

PC mit UAExpert

1. Starten Sie „UAExpert“.
2. Öffnen Sie das Projekt mit den aktuellen Einstellungen.
3. Öffnen Sie im Projektbaum unter „**Project**“ > „**Servers**“ das Kontextmenü des WAGO-OPC-UA-Servers mit der rechten Maustaste.
4. Wählen Sie den Menüpunkt „**Properties**“ aus.
5. Überprüfen Sie die folgenden Einstellungen und passen Sie sie ggf. an.

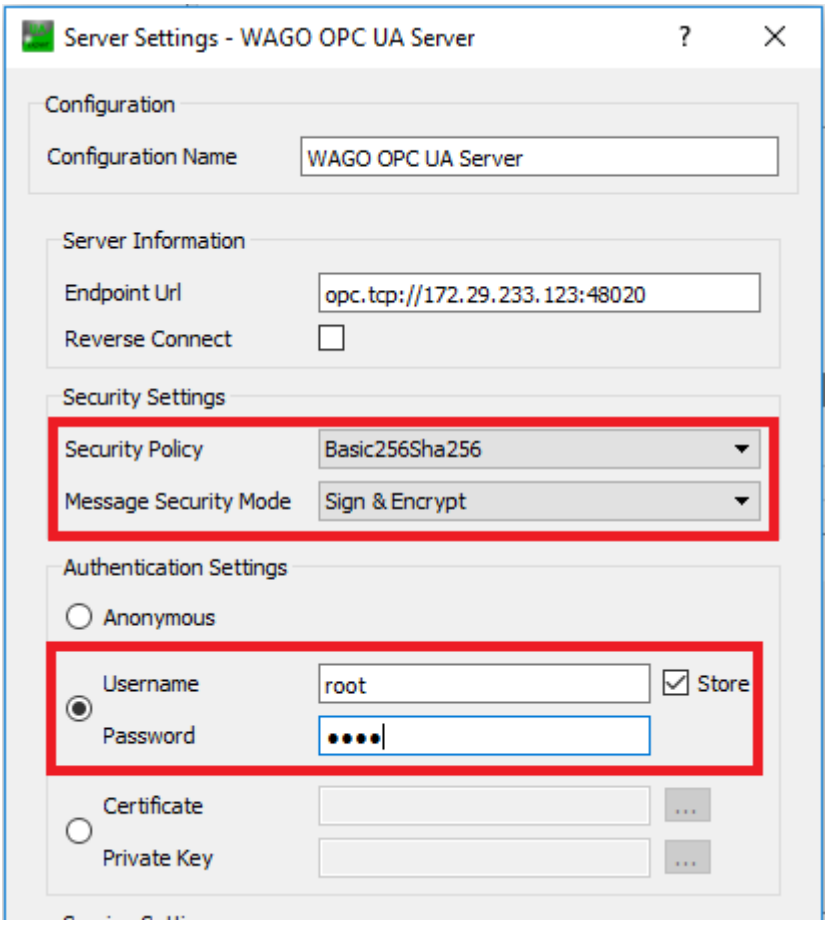

Abbildung 6: Verbindungseinstellungen

Für den Zertifikatsaustausch ist in „UAExpert“ eine spezielle Sicht vorhanden (GDS Push View). Mit einer Verbindung zum Server kann in dieser Sicht ein neues Serverzertifikat erstellt werden. Es können auch Zertifikate, die von einer anderen Stelle erzeugt worden sind, geladen werden.

Um diese Sicht zu öffnen, gehen Sie folgendermaßen vor:

PC mit UAExpert

6. Öffnen Sie im Projektbaum unter „**Project**“ das Kontextmenü des Eintrags „**Documents**“ mit der rechten Maustaste.

7. Wählen Sie den Menüpunkt „**Add …**“ aus.

→ Das Dialogfenster „**Add Document**“ wird geöffnet.

8. Wählen Sie im Auswahlfeld „**Document Type**“ den Wert „GDS Push View“ aus.

9. Klicken Sie die Schaltfläche **[Add]**, um das Dialogfenster zu schließen und die Sicht anzulegen.

→ Das folgende Register wird geöffnet (Abb. „GDS Push View“).

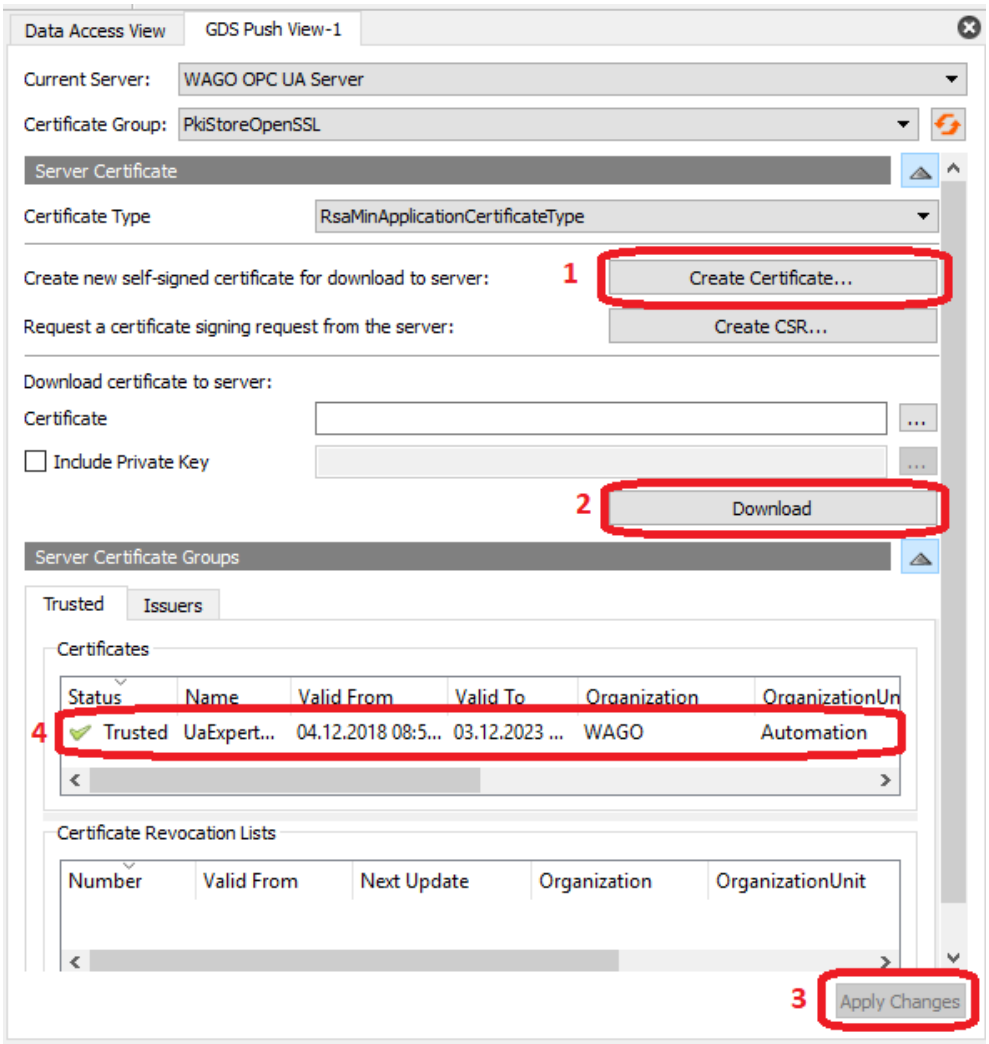

Abbildung 7: GDS Push View

Wenn ein Zertifikat durch „UaExpert“ erneuert wird, so muss dieses Zertifikat erzeugt, vom Server signiert und auf den Server heruntergeladen werden.

10. Klicken Sie die Schaltfläche **[Create Certificate …]**, um ein neues Zertifikat zu erzeugen (Abb. „GDS Push View“, Bereich 1).

→ Das folgende Dialogfenster wird angezeigt:

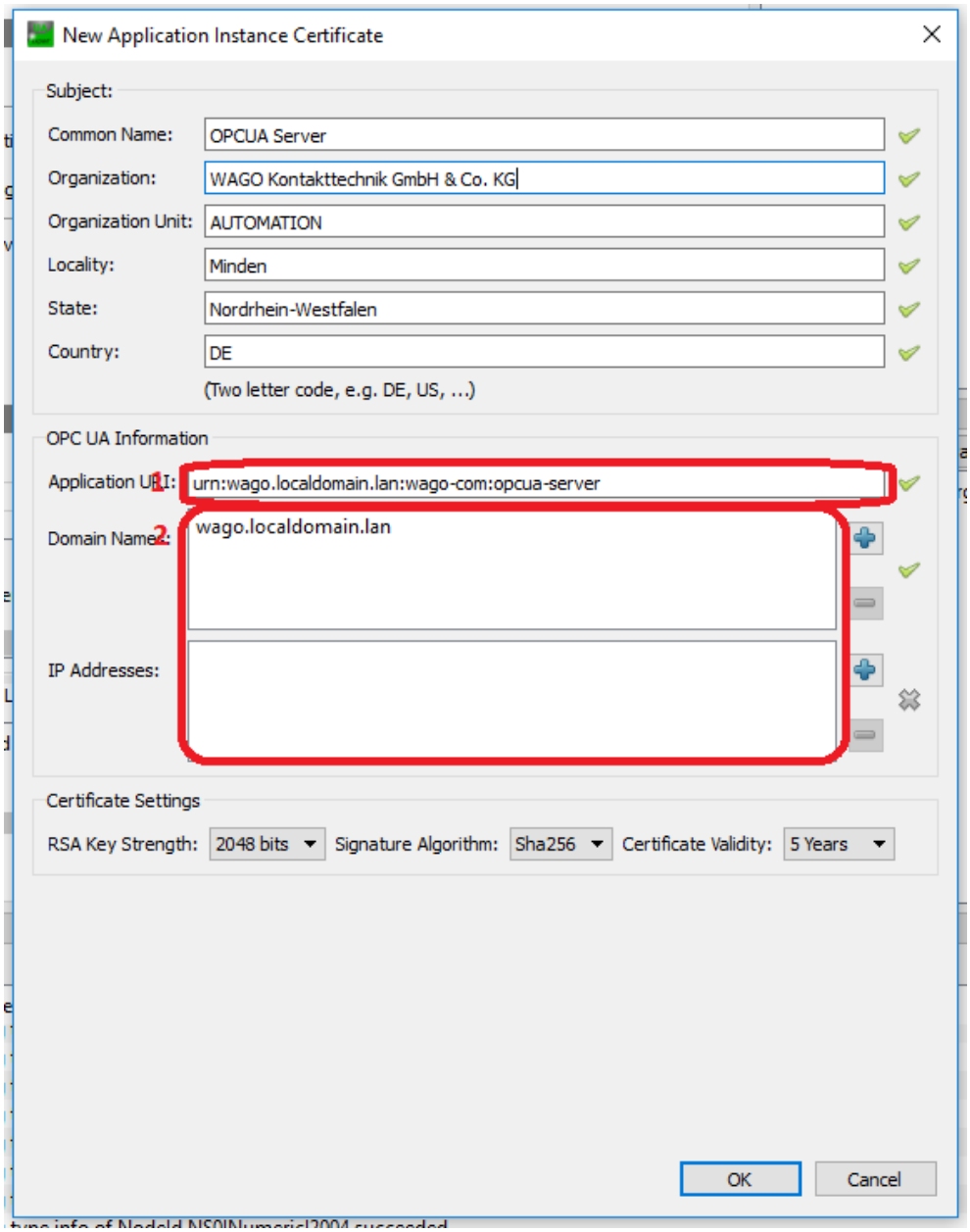

Abbildung 8: Zertifikatseinstellungen

Die Voreinstellungen, die in diesem Dialogfenster angezeigt werden, wurden zuvor aus dem aktuellen, auf dem Gerät verwendeten Zertifikat gelesen.

11. Passen Sie die „Application URI“ an das vorhandene Umfeld an (Abb. „Zertifikatseinstellungen“, Bereich 1). Das benötigte Format ist: „urn:[Hostname].[Domain Name]:wago-com:opcua-server“.

12. Ergänzen Sie die Verbindungsinformationen über „Domain Name“ oder „IP Addresses“ (Abb. „Zertifikatseinstellungen“, Bereich 2). In der Abbildung ist beispielhaft die Verbindungsinformation als Hostname und Domainname hinzugefügt worden. Es ist auch die Verwendung einer IP-Adresse möglich.

13. Klicken Sie die Schaltfläche **[OK]**, um die Eingaben zu speichern und das Dialogfenster zu schließen.

14. Klicken Sie im Register „GDS Push View“ die Schaltfläche **[Download]**, um das Zertifikat in den Controller zu laden (Abb. „GDS Push View“, Bereich 2).

→ Ein Meldungsfenster mit einer Abfrage wird geöffnet.

15. Klicken Sie die Schaltfläche **[No]**, um das Zertifikat unverändert zu übernehmen und das Meldungsfenster zu schließen.

→ Ein weiteres Meldungsfenster mit einer Erinnerung wird geöffnet.

16. Klicken Sie die Schaltfläche **[OK]**, um die Erinnerung zu quittieren und dieses Meldungsfenster zu schließen.

17. Klicken Sie die Schaltfläche **[Apply Changes]**, um das in den Controller geladene Zertifikat zu aktivieren (Abb. „GDS Push View“, Bereich 3).

→ Nach der Aktivierung bricht die aktuelle Verbindung vom Server zum Client ab, da das aktuell vom Server verwendete Zertifikat nicht mehr mit dem in der Verbindung verwendeten Zertifikat übereinstimmt.

18. Öffnen Sie im Projektbaum unter „**Project**“ > „**Servers**“ das Kontextmenü des WAGO-OPC-UA-Servers mit der rechten Maustaste.

19. Wählen Sie den Menüpunkt „**Disconnect**“ aus, um die Verbindung zu trennen.

20. Öffnen Sie im Projektbaum unter „**Project**“ > „**Servers**“ das Kontextmenü des WAGO-OPC-UA-Servers mit der rechten Maustaste.

21. Wählen Sie den Menüpunkt „**Connect**“ aus, um die Verbindung wiederherzustellen.

→ Wenn die Verbindung nun nicht mehr möglich ist, kontrollieren sie die Einstellung aus Abb. „OPCUA-Einstellungen im Web-based-Management“.

→ Wenn die Verbindung wiederaufgebaut wird, so wird das Zertifikat angezeigt, das für den aktuellen Verbindungaufbau verwendet wird (Abb. „GDS Push View“, Bereich 4).

22. Öffnen Sie das Kontextmenü dieses Zertifikatseintrags mit der rechten Maustaste.

23. Wählen Sie den Menüpunkt „**Trust**“.

→ Das Zertifikat wird nun zu der Liste der vertrauenswürdigen Zertifikate hinzugefügt.

Wenn Sie weitere Server-Client-Konstellationen zulassen wollen, führen Sie für diese Konstellationen einen erneuten Verbindungsversuch durch.
Dieser Versuch wird fehlschlagen, da das Client-Zertifikat nicht akzeptiert ist.
Die Verbindung kann nach dem gescheiterten Versuch einer akzeptierten Server-Client-Konstellation hinzugefügt werden. Gehen Sie dazu wie oben beschrieben vor.

7.2 OPC-UA-Clients hinzufügen

In diesem Abschnitt werden die Schritte beschrieben, welche durchzuführen sind, um weitere Clients für den Verbindungsaufbau zu einem OPC-UA-Server hinzuzufügen.

Voraussetzung:

- UaExpert mit Version >= 1.4.4.
- Ein Controller PFC100 oder PFC200 mit laufendem OPC-UA-Server
- Zertifikate für die weiteren Clients

Hinweis

Die Erstinbetriebnahme für Zertifikate muss abgeschlossen sein!
Verwenden Sie für das Hinzufügen von OPC-UA-Clients den Client (z. B. UAExpert), mit dem die Erstinbetriebnahme durchgeführt wurde, da für diese Konstellation bereits ein Zertifikat erstellt wurde.

Erläuterung:

Es gibt verschiedenen Möglichkeiten, Clients hinzuzufügen.

- Ein Client versucht sich auf den Server zu verbinden, und wird abgelehnt. Das Zertifikat befindet sich somit im Bereich der nicht akzeptierten Zertifikate. Über einen vertrauenswürdigen Client wird die Verbindung als vertrauenswürdig (Trust) hinzugefügt.

- Ein Client-Zertifikat wird über eine vertrauenswürdige Verbindung auf den Server geladen.

Hier wird nur die Vorgehensweise für das Hinzufügen über zwei Clients beschrieben.

PC mit hinzuzufügendem OPC-UA-Client

1. Starten Sie UaExpert auf dem hinzuzufügenden Client.

2. Öffnen Sie in dem Fenster „Project“ den Baum „Project/Servers“.

3. Öffnen Sie mit der rechten Maustaste auf „Server“ das Kontextmenü.

4. Wählen Sie den Menüpunkt „Add …“ aus.

5. Geben Sie unter „Configuration Name“ einen sprechenden Namen für den Server ein (z. B. „WAGO OPC-UA-Server“).

6. Wählen Sie das Register „Advanced“ aus.

7. Geben Sie in der Gruppe „Server Information“ im Feld „Endpoint Url“ die Verbindung zum Server ein (z. B. „opc.tcp://172.29.233.206“).

8. Wählen Sie in der Gruppe „Security Settings“ im Auswahlfeld „Security Policy“ den Eintrag „Basic256Sha256“ und im Auswahlfeld „Message Security Mode“ den Eintrag „Sign & Encrypt“ aus.

9. Wählen Sie in der Gruppe „Authentication Settings“ die Option „Username/Password“ aus.

10. Geben Sie im Feld „**Username**“ den Benutzernamen „root“ und im Feld „**Password**“ das Passwort ein (im Auslieferungszustand „wago“).

11. Markieren Sie das Kontrollfeld „Store“ und schließen Sie das Fenster mit **[OK]**.

12. Öffnen Sie in dem Fenster „Project“ den Baum „Project/Servers“.

13. Öffnen Sie mit der rechten Maustaste das Kontextmenü des gerade angelegten Servers.

14. Wählen Sie den Menüpunkt „Connect“ aus.

→ Es kann noch keine Verbindung aufgebaut werden.

PC mit vertrauenswürdigem OPC-UA-Client

15. Starten Sie UaExpert auf dem vertrauenswürdigen Client.

16. Öffnen Sie in dem Fenster „Project“ den Baum „Project/Servers“.

17. Öffnen Sie mit der rechten Maustaste das Kontextmenü des gewünschten Servers.

18. Wählen Sie den Menüpunkt „Connect“ aus.

19. Öffnen Sie in dem Fenster „Project“ den Baum „Project/Documents“.

20. Wählen Sie den Menüpunkt „Add …“ aus.

21. Wählen Sie in der Gruppe „Document Type“ den Eintrag „GDS Push View“ aus.

22. Schließen Sie das Fenster mit **[Add]**.

23. Wählen Sie im Register „GDS Push View“ im Auswahlfeld „Current Server“ den gewünschten Server aus.

→ In der Gruppe „Server Certificate Groups“ im Register „Trusted“ wird das Zertifikat aus dem zuvor getätigten Verbindungsversuch als „Untrusted“ angezeigt.

24. Öffnen Sie mit der rechten Maustaste das Kontextmenü dieses Zertifikats.

25. Wählen Sie den Menüpunkt „Trust“ aus.

→ Das Zertifikat wird nun als „Trusted“ angezeigt.

26. Öffnen Sie in dem Fenster „Project“ den Baum „Project/Servers“.

27. Öffnen Sie mit der rechten Maustaste das Kontextmenü des gerade angelegten Servers.

28. Wählen Sie den Menüpunkt „Disconnect“ aus.

→ Die Verbindung zum Server wird abgebrochen.

Abbildungsverzeichnis

Abbildung 1: Oberfläche des UAExpert 21
Abbildung 2: Hinzufügen eines Servers 22
Abbildung 3: Bestätigung des Server-Zertifikats 23
Abbildung 4: Meldung bei Verbindungsaufbau 24
Abbildung 5: Meldung bei Verbindungsaufbau 26
Abbildung 6: Verbindungseinstellungen 34
Abbildung 7: GDS Push View 35
Abbildung 8: Zertifikatseinstellungen 36

Tabellenverzeichnis

Tabelle 1: Darstellungen der Zahlensysteme 8
Tabelle 2: Schriftkonventionen 8
Tabelle 3: Teile des OPC-UA-Servers 16
Tabelle 4: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Server“ 28
Tabelle 5: WBM-Seite „OPC UA Configuration“ – Gruppe „General OPC UA Server Configuration“ 29
Tabelle 6: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Endpoints“ 30
Tabelle 7: WBM-Seite „OPC UA Configuration“ – Gruppe „OPC UA Security Settings“ 31
Tabelle 8: WBM-Seite „OPC UA Information Model“ – Gruppe „OPC UA Server Information Model“ 32

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Telefax: 0571/887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com