



ibaPDA-OPC-UA-Server+

OPC UA-Server für Messdaten

Handbuch
Ausgabe 1.2

Messsysteme für Industrie und Energie
www.iba-ag.com

Hersteller

iba AG
Königswarterstr. 44
90762 Fürth
Deutschland

Kontakte

Zentrale	+49 911 97282-0
Telefax	+49 911 97282-33
Support	+49 911 97282-14
Technik	+49 911 97282-13
E-Mail	iba@iba-ag.com
Web	www.iba-ag.com

Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts sind nicht gestattet, soweit nicht ausdrücklich zugestanden. Zuwiderhandlungen verpflichten zu Schadenersatz.

© iba AG 2022, alle Rechte vorbehalten.

Der Inhalt dieser Druckschrift wurde auf Übereinstimmung mit der beschriebenen Hard- und Software überprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass für die vollständige Übereinstimmung keine Garantie übernommen werden kann. Die Angaben in dieser Druckschrift werden jedoch regelmäßig aktualisiert. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten oder können über das Internet heruntergeladen werden.

Die aktuelle Version liegt auf unserer Website www.iba-ag.com zum Download bereit.

Version	Datum	Revision - Kapitel / Seite	Autor	Version SW
1.2	01-2022	Hinweis Aktualisierungszyklus; writable Tags; zentr. Zertifikatspeicher	RM	7.2.0

Windows® ist eine Marke und eingetragenes Warenzeichen der Microsoft Corporation. Andere in diesem Handbuch erwähnte Produkt- und Firmennamen können Marken oder Handelsnamen der jeweiligen Eigentümer sein.

Inhalt

1	Zu diesem Handbuch.....	4
1.1	Zielgruppe und Vorkenntnisse.....	4
1.2	Schreibweisen.....	4
1.3	Verwendete Symbole.....	5
2	Systemvoraussetzungen	6
3	OPC UA-Server und OPC UA-Server+.....	7
3.1	Allgemeine Informationen.....	7
3.2	Systemtopologien	8
4	Konfiguration und Projektierung ibaPDA	9
4.1	OPC UA Server – Konfiguration.....	11
4.2	Zertifikate.....	15
4.2.1	Einleitung.....	15
4.2.2	Zentraler Zertifikatspeicher	16
4.2.3	Zertifikate verwalten.....	18
4.2.3.1	Ein neues Zertifikat erzeugen	19
4.2.3.2	Zertifikat hinzufügen.....	20
4.2.3.3	Zertifikate exportieren.....	20
4.2.4	Zertifikate verwenden.....	21
4.2.5	Speichern und Schützen von Zertifikaten	22
4.3	OPC UA Server – Tags	23
4.3.1	Standard-Tags	26
4.3.2	Erfasste Signale (Modules)	28
4.3.3	Writable Tags	29
4.3.4	Benutzerdefinierte Informationsmodelle	31
5	Diagnose	34
5.1	Lizenz	34
5.2	Register Diagnose	35
5.3	Verbindungsdiagnose mittels PING	36
6	Support und Kontakt	37

1 Zu diesem Handbuch

Diese Dokumentation beschreibt die Funktion und die Anwendung der Software

ibaPDA-OPC-UA-Server+.

1.1 Zielgruppe und Vorkenntnisse

Diese Dokumentation wendet sich an ausgebildete Fachkräfte, die mit dem Umgang mit elektrischen und elektronischen Baugruppen sowie der Kommunikations- und Messtechnik vertraut sind. Als Fachkraft gilt, wer auf Grund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Bestimmungen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann.

Im Besonderen wendet sich diese Dokumentation an Personen, die mit Projektierung, Test, Inbetriebnahme oder Instandhaltung der verwendeten Speicherprogrammierbaren Steuerungen und Kommunikationssysteme befasst sind. Für den Umgang mit *ibaPDA-OPC-UA-Server+* sind folgende Vorkenntnisse erforderlich bzw. hilfreich:

- Betriebssystem Windows
- Grundkenntnisse *ibaPDA*
- Kenntnis der Konfiguration eines OPC UA-Servers

1.2 Schreibweisen

In dieser Dokumentation werden folgende Schreibweisen verwendet:

Aktion	Schreibweise
Menübefehle	Menü <i>Funktionsplan</i>
Aufruf von Menübefehlen	<i>Schritt 1 – Schritt 2 – Schritt 3 – Schritt x</i> Beispiel: Wählen Sie Menü <i>Funktionsplan – Hinzufügen – Neuer Funktionsblock</i>
Tastaturtasten	<Tastename> Beispiel: <Alt>; <F1>
Tastaturtasten gleichzeitig drücken	<Tastename> + <Tastename> Beispiel: <Alt> + <Strg>
Grafische Tasten (Buttons)	<Tastename> Beispiel: <OK>; <Abbrechen>
Dateinamen, Pfade	"Dateiname", "Pfad" Beispiel: "Test.doc"

1.3 Verwendete Symbole

Wenn in dieser Dokumentation Sicherheitshinweise oder andere Hinweise verwendet werden, dann bedeuten diese:

Gefahr!



Wenn Sie diesen Sicherheitshinweis nicht beachten, dann droht die unmittelbare Gefahr des Todes oder der schweren Körperverletzung!

- Beachten Sie die angegebenen Maßnahmen.
-

Warnung!



Wenn Sie diesen Sicherheitshinweis nicht beachten, dann droht die mögliche Gefahr des Todes oder schwerer Körperverletzung!

- Beachten Sie die angegebenen Maßnahmen.
-

Vorsicht!



Wenn Sie diesen Sicherheitshinweis nicht beachten, dann droht die mögliche Gefahr der Körperverletzung oder des Sachschadens!

- Beachten Sie die angegebenen Maßnahmen.
-

Hinweis



Hinweis, wenn es etwas Besonderes zu beachten gibt, wie z. B. Ausnahmen von der Regel usw.

Tipp



Tipp oder Beispiel als hilfreicher Hinweis oder Griff in die Trickkiste, um sich die Arbeit ein wenig zu erleichtern.

Andere Dokumentation



Verweis auf ergänzende Dokumentation oder weiterführende Literatur.

2 Systemvoraussetzungen

Folgende Systemvoraussetzungen gelten für die Verwendung der OPC UA Server+:

- *ibaPDA v7.0.0* oder höher
- Lizenz für *ibaPDA-OPC-UA-Server+*
- Netzwerkverbindung zu einem oder mehreren OPC UA-Client

Andere Dokumentation



Sonstige Voraussetzungen, wie die eingesetzte PC-Hardware und die unterstützten Betriebssysteme, entnehmen Sie der *ibaPDA*-Dokumentation.

Hinweis



Es wird empfohlen, die OPC UA-Kommunikation zur Datenerfassung auf einem separaten Netzwerk abzuwickeln, um eine Beeinflussung der OPC UA-Telegramme durch den Ethernet-Datenverkehr zwischen *ibaPDA* und anderen Knoten im Netzwerk (Dateiserver, Messdateianforderungen usw.) zu vermeiden.

Lizenzinformationen

Bestell-Nr.	Produktbezeichnung	Beschreibung
30.670051	ibaPDA-OPC-UA-Server+	Erweiterungslizenz für ein <i>ibaPDA</i> -System um die Funktion: OPC UA Server+

Tab. 1: Verfügbare OPC UA-Server+Lizenzen

3 OPC UA-Server und OPC UA-Server+

3.1 Allgemeine Informationen

ibaPDA bietet bei OPC UA standardmäßig die Funktion als OPC UA-Server, um Daten und Informationen über den eigenen Status öffentlich zur Verfügung zu stellen. Es handelt sich um Informationen wie z. B.

- Version
- Aktivierte Lizenzen
- Status der Datenerfassung und -aufzeichnung
- Verbunden OPC UA-Clients

Die OPC UA-Server-Funktion ist damit eine Alternative zur SNMP-Schnittstelle oder dem Watchdog-Telegramm, um anderen Systemen Informationen über den Status von *ibaPDA* mitzuteilen.

Mit der Erweiterung *ibaPDA-OPC-UA-Server+* haben Sie die Möglichkeit, auch sämtliche erfassten oder berechneten Signale sowie Textkanäle über OPC UA zu veröffentlichen.

Somit können andere Systeme mit OPC UA-Client-Funktion auf die von *ibaPDA* erfassten Daten zugreifen.

Die Auswahl der Signale, die via OPC UA publiziert werden, erfolgt komfortabel anhand des Signalbaums im I/O-Manager von *ibaPDA*.

Die Aktualisierung der Signalwerte erfolgt zyklisch.

Hinweis



Die Tags im OPC UA-Server werden wie die Ausgänge von *ibaPDA* aktualisiert. Der schnellste Aktualisierungszyklus ergibt sich also aus dem kleinsten gemeinsamen Vielfachen aller Modulzeitbasen, bzw. beträgt mindestens 50 ms.

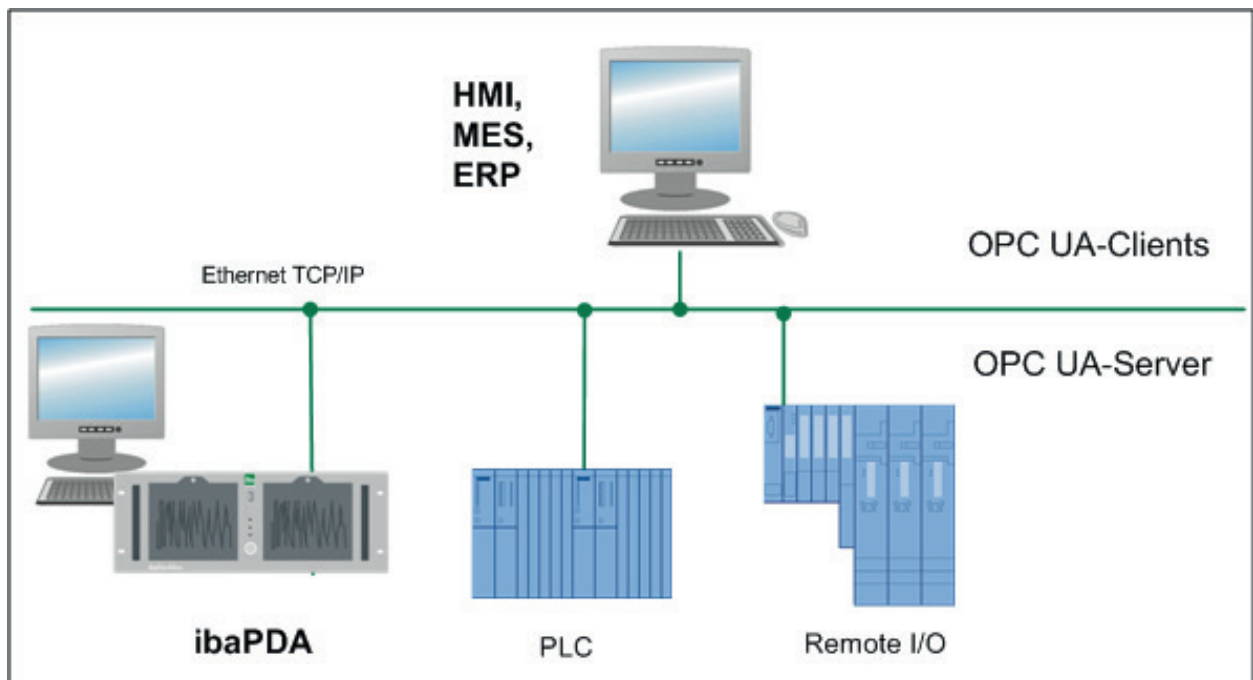
Die standardmäßig von *ibaPDA* als OPC UA-Server bereitgestellten Tags können von OPC UA-Clients nur gelesen aber nicht geschrieben werden.

Sie können aber bei Bedarf sog. *Writable Tags* (analog und digital) im Datenmodell des OPC UA-Servers hinzufügen. Mithilfe eines *OPC UA-Server-Moduls*, das Sie unter dem Schnittstellenknoten *OPC UA* hinzufügen, können OPC UA-Clients auch Werte im *ibaPDA* OPC UA-Server beschreiben. Für die Nutzung von *Writable Tags* und *OPC UA-Server-Modul* benötigen Sie ebenfalls die Zusatzlizenz *ibaPDA-OPC-UA-Server+*.

Die für die Kommunikation zwischen OPC-UA-Server (*ibaPDA*) und einem OPC-UA-Client erforderlichen Zertifikate können in *ibaPDA* importiert oder generiert werden.

3.2 Systemtopologien

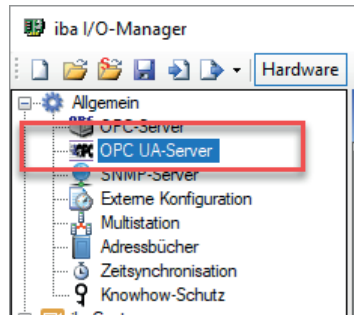
Die folgende Abbildung gibt einen Überblick über eine mögliche Konfiguration.



4 Konfiguration und Projektierung ibaPDA

Öffnen Sie den I/O-Manager, z. B. mithilfe der Symbolleiste .

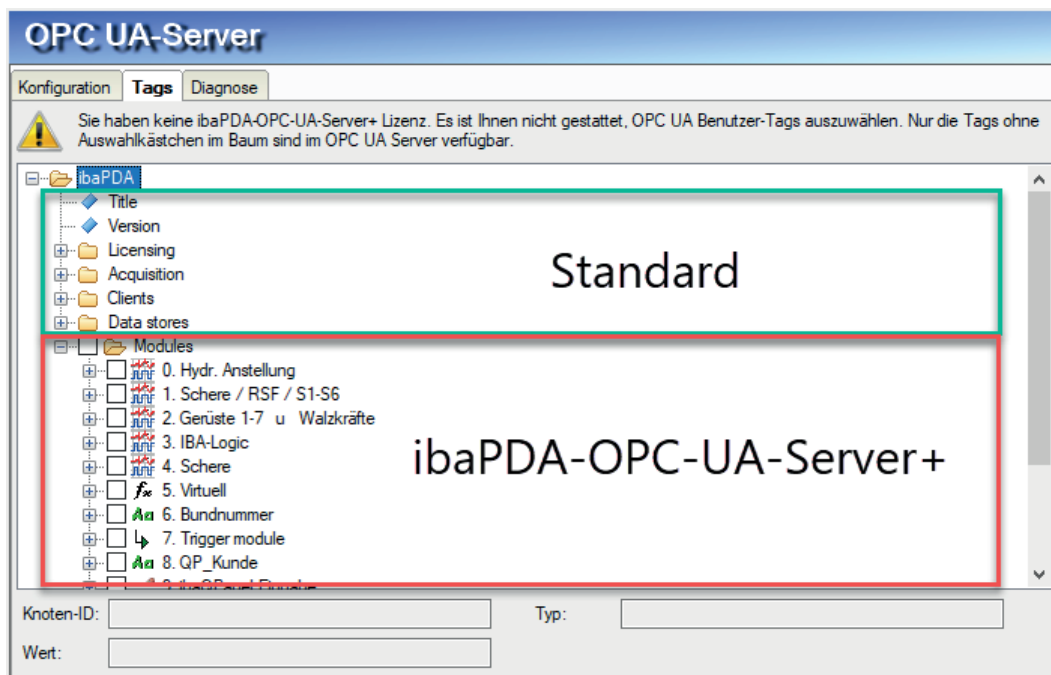
In dem Signalbaum gibt es unter *Allgemein* den Knoten *OPC UA-Server*.



Markieren Sie den Knoten und wählen Sie dann rechts daneben das Register *Tags*.

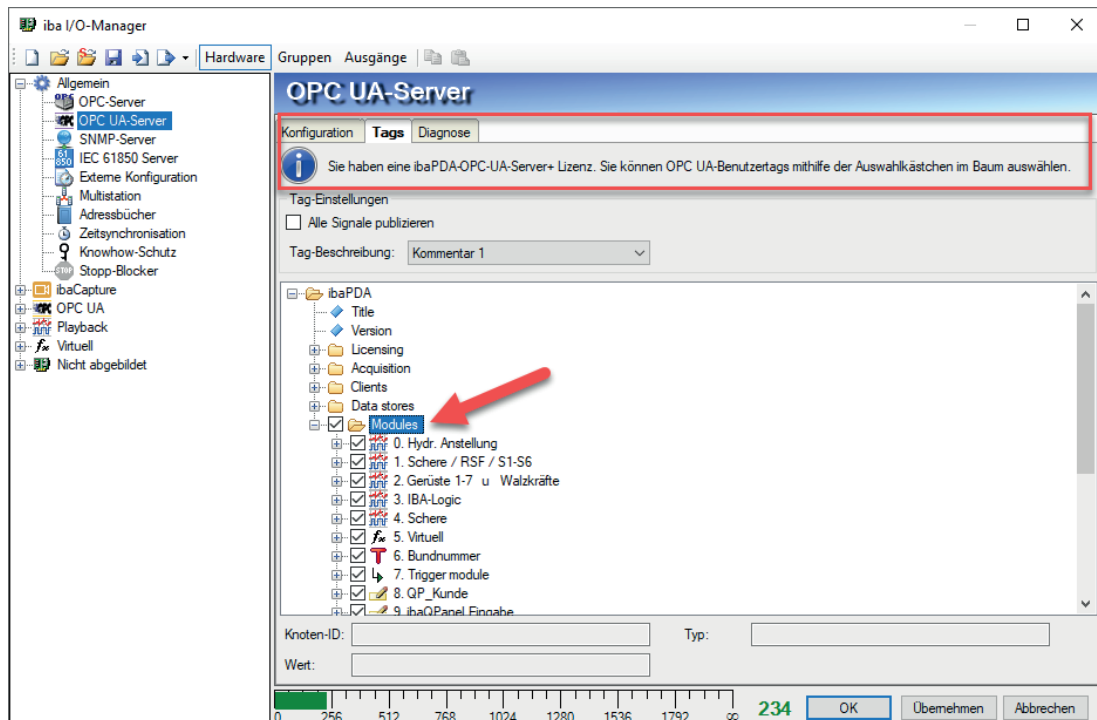
In dem Register sehen Sie einen Signalbaum mit den Tags, die *ibaPDA* zur Verfügung stellt. Die Tags, die in der Standardversion verfügbar sind, haben keine Auswahlkästchen.

Die Signale bzw. Tags unter dem Knoten *Module* haben Auswahlkästchen und können nur mit der Lizenz *ibaPDA-OPC-UA-Server+* genutzt werden.



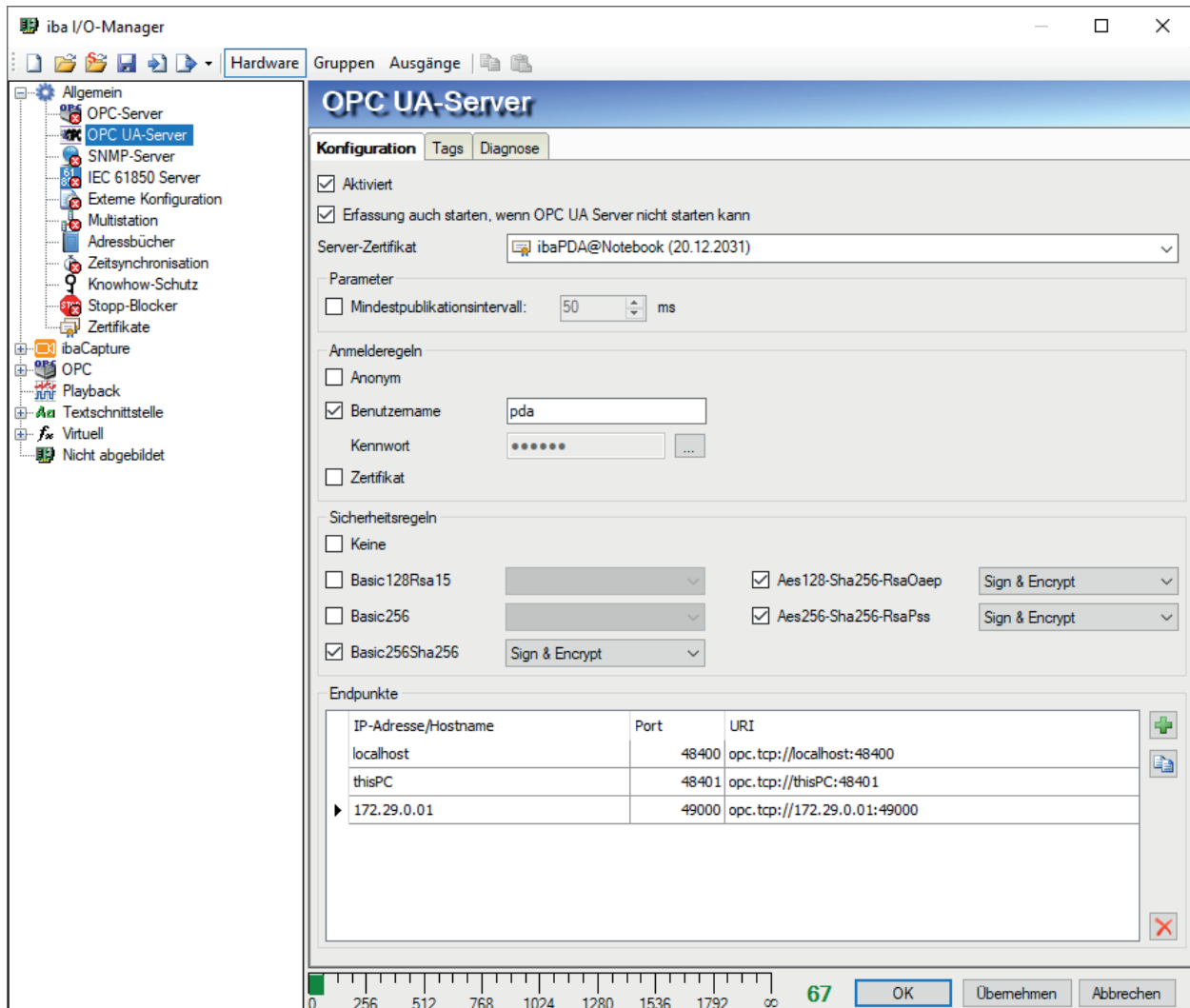
Wenn in Ihrem Dongle die OPC UA Server+-Funktion nicht aktiviert ist, dann steht oben im Register ein Hinweis.

Wenn in Ihrem Dongle die OPC UA Server+-Funktion aktiviert ist, dann finden Sie in dem Register einen entsprechenden Hinweis und Sie können Häkchen in die Auswahlkästchen setzen, um Signale auszuwählen.



4.1 OPC UA Server – Konfiguration

Im Register *Konfiguration* müssen Sie den OPC UA Server zunächst aktivieren, um weitere Einstellungen vornehmen zu können.



Aktiviert

Setzen Sie hier ein Häkchen, um die OPC-UA-Server-Funktion zu aktivieren.

Erfassung auch starten, wenn OPC UA-Server nicht starten kann

Wenn diese Option aktiviert ist, startet die Erfassung auch dann, wenn der OPC UA-Server nicht gestartet werden kann. Im Prüfungsdialog wird eine Warnung ausgegeben. Wenn das System ohne OPC UA-Server gestartet wurde, dann versucht *ibaPDA* in regelmäßigen Abständen, den OPC UA Server zu starten. Solange der OPC UA-Server nicht gestartet wurde, werden keine OPC UA-Tags publiziert und *ibaPDA* ist als OPC UA-Server im Netzwerk nicht sichtbar.

Server-Zertifikat

Wählen Sie hier aus der Drop-down-Liste das Zertifikat aus, das der OPC UA-Server nutzen soll.

Falls Sie noch kein Zertifikat erzeugt oder importiert haben, können Sie das tun, indem Sie aus der Liste den Eintrag *Neues Zertifikat erzeugen* oder *Zertifikate verwalten* auswählen.

Sie werden dann zum zentralen Zertifikatspeicher umgeleitet, den Sie auch im Schnittstellenbaum unter *Allgemein - Zertifikate* finden.

Der Umgang mit den Zertifikaten ist in Kapitel [↗ Zertifikate](#), Seite 15 , beschrieben.

Parameter

Bei Bedarf können Sie hier das Publikationsintervall des OPC UA-Servers anpassen.

Wenn Sie diese Option nicht aktivieren (Default), richtet sich das Publikationsintervall wie bei allen anderen Ausgangsschnittstellen nach dem kleinsten gemeinsamen Vielfachen aller Modulzeitbasen und beträgt minimal 50 ms.

Wenn Sie diese Option aktivieren, dann können Sie das Publikationsintervall auf einen höheren Wert einstellen, z. B. 500 ms. Damit wird sichergestellt, dass der OPC UA-Server nicht schneller als alle 500 ms seine Tags publiziert, auch wenn eine höhere Publikationsrate seitens der Clients gefordert ist.

Damit kann z. B. einer Überlastung der Kommunikationsbandbreite entgegengewirkt werden, wenn viele OPC UA-Clients große Datenmengen vom Server anfordern.

Anmelderegeln

Mindestens eine der folgenden Anmelderegeln sollte eingestellt werden:

Anonym

Wenn diese Option aktiviert ist, dann können sich Clients am OPC UA Server ohne Anmeldeinformationen (Benutzer/Kennwort) anmelden.

Benutzername/Kennwort

Wenn diese Option aktiviert ist, können sich Clients nur anmelden, wenn sie sich mit Benutzername und Kennwort, die hier im Dialog eingetragen wurden, authentifizieren können.

Mit Klick auf den  Button wird das Kennwort vorübergehend lesbar angezeigt.

Zertifikat

Wenn diese Option aktiviert ist, können sich Clients anmelden, wenn sie ein bestätigtes Zertifikat verwenden.

Sicherheitsregeln

Mindestens eine der Optionen muss aktiviert werden.

Wenn Sie die Option *Keine* aktivieren, dann werden auch Verbindungen ohne Verschlüsselung (Encryption) unterstützt.

Zu jeder der anderen Optionen bzw. Verschlüsselungen können Sie jeweils eine Sicherheitsregel mit Signatur und/oder Verschlüsselung auswählen:

- Sign
- Sign & encrypt
- Sign + Sign & Encrypt

Hinweis

Die Verschlüsselungen Basic128Rsa15 und Basic256 sind inzwischen veraltet. Aus Sicherheitsgründen ist die Verwendung der Verschlüsselungen Basic-256Sha256, Aes128-Sha256-RsaOaep oder Aes256-Sha256-RsaPss zu bevorzugen.

Endpunkte

In diesem Teil des Dialogs können Sie konfigurieren, welche lokalen Endpunkten der Server bereitstellt.

Ein Endpunkt ist eine Kombination aus IP-Adresse und Portnummer. Anstatt eine spezifische IP-Adresse einzugeben, ist es auch möglich, den Rechnernamen des OPC UA-Servers einzugeben. Das gilt für alle IP-Adressen aller Netzwerkschnittstellen im System. Aus IP-Adresse oder Rechnername und der Portnummer wird ein sog. URI (Uniform Resource Identifier) gebildet.

Endpunkte			
IP-Adresse/Rechnername	Port	URI	
thisPC	48400	opc.tcp://thisPC:48400	
thisPC	48401	opc.tcp://thisPC:48401	
I 172.29.0.101	49000	opc.tcp://172.29.0.101:49000	


In dem Beispiel in der Abbildung oben können sich OPC UA-Clients von jedem Netzwerk aus mit dem OPC UA-Server verbinden, wenn sie Port 48400 oder 48401 nutzen. Darüber hinaus können Clients außerdem eine Verbindung zur IP-Adresse 172.29.0.101 über Port 49000 aufbauen.

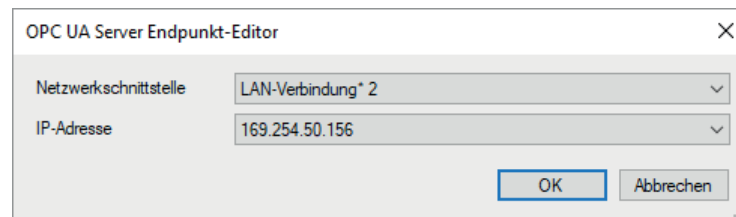
Die Liste der Endpunkte bietet einige Bedienelemente:

Button	Funktion
	Mit diesem Button fügen Sie einen neuen Endpunkt hinzu. Der neue Endpunkt hat zunächst stets die gleichen Daten wie der lokale Rechner und muss anschließend bearbeitet werden.
	Mit diesem Button duplizieren Sie einen gewählten Endpunkt, den Sie anschließend bearbeiten können.
	Mit diesem Button entfernen Sie den gewählten Endpunkt aus der Liste.

Tab. 2: Bedienelemente der Endpunktliste

Standardmäßig ist bereits der Rechnername des lokalen Rechners in der Liste eingetragen.

Wenn Sie einen Endpunkt in der Liste anklicken, erscheint der Button . Klicken Sie auf diesen Button, um den Endpunkt zu bearbeiten.



Stellen Sie die gewünschte Netzwerkschnittstelle ein, über die die OPC UA-Clients kommunizieren sollen. Die Auswahlliste zeigt alle in dem Rechner verfügbaren Netzwerkschnittstellen mit all ihren IP-Adressen.

Klicken Sie auf <OK> und die gewählte IP-Adresse wird in der Liste angezeigt.

Hinweis



Zurzeit werden nur IPv4-Adressen unterstützt.

4.2 Zertifikate

Die Kommunikation des OPC UA-Servers wird über Zertifikate abgesichert. Die Verwaltung der Zertifikate erfolgt in *ibaPDA* im zentralen Zertifikatspeicher, wo neben den Zertifikaten für die OPC UA-Kommunikation auch andere Zertifikate, z. B. für Schnittstellen und Datenaufzeichnungen zu finden sind.

4.2.1 Einleitung

Für eine sichere, verschlüsselte TLS/SSL-Kommunikation zwischen einem Client und einem Server werden sog. Zertifikate verwendet, da mit ihnen eine sichere Authentifizierung möglich ist.

Bevor sich ein Client mit einem Server verbinden kann, muss zunächst ein Anwendungszertifikat konfiguriert werden. Zertifikate können sowohl von Server- als auch von Clientseite zur Verfügung gestellt werden. Eine Kommunikation kann nur dann erfolgen, wenn jeder Partner dem Partnerzertifikat vertraut.

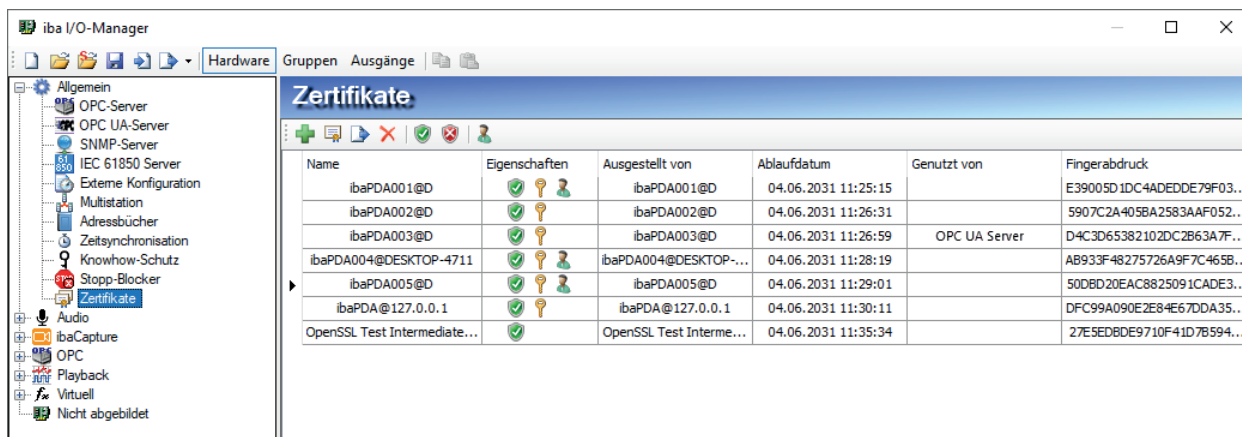
Zertifikate können entweder beim Verbindungsaufbau spontan ausgetauscht oder im Vorfeld als vertrauenswürdig registriert werden. Wird ein bislang unbekanntes Zertifikat bei einem Verbindungsaufbau angeboten, so muss interaktiv durch den Anwender das Zertifikat akzeptiert oder abgelehnt werden. Akzeptierte Zertifikate werden automatisch in die Tabelle des *Zertifikatspeichers* eingetragen und als vertrauenswürdig gekennzeichnet. Wenn das Zertifikat abgelehnt wird, dann findet kein Kommunikationsaufbau statt.

Sie können Zertifikate auch registrieren und dann als „nicht vertrauenswürdig“ kennzeichnen. Eine Kommunikation zu einem Partner mit solch einem Zertifikat wird dann grundsätzlich abgelehnt. Wenn Zertifikate erst einmal registriert, d. h. in der Tabelle des Zertifikatspeichers eingetragen sind, dann wird der Anwender beim Kommunikationsaufbau nicht mehr benachrichtigt bzw. gefragt – egal, ob die Zertifikate als „vertrauenswürdig“ oder „nicht vertrauenswürdig“ gekennzeichnet sind.

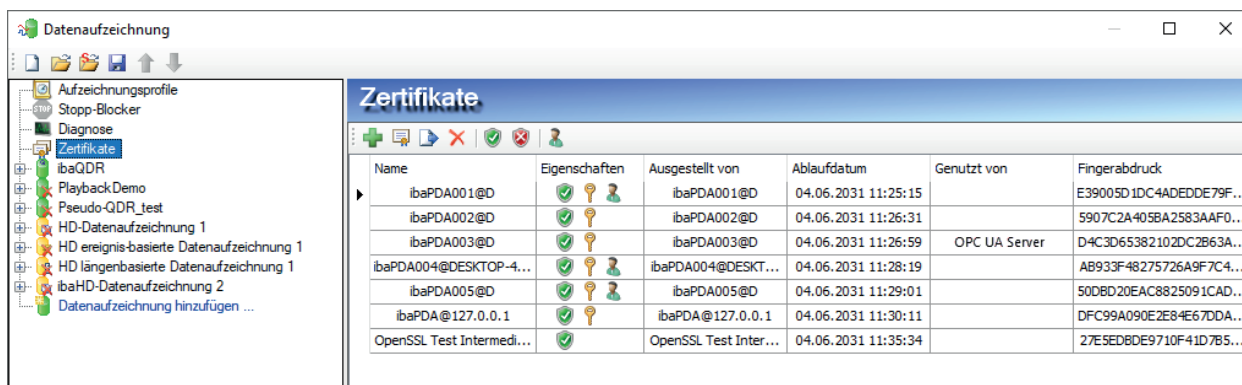
Einige Schnittstellen in *ibaPDA*, wie z. B. die E-Mail-Ausgabe, nutzen Windows-Zertifikate. Andere Funktionen, wie z. B. OPC UA-Server oder MQTT-Datenaufzeichnung nutzen Zertifikate aus dem zentralen Zertifikatspeicher von *ibaPDA*.

4.2.2 Zentraler Zertifikatspeicher

Alle registrierten Zertifikate sind in einer Tabelle aufgelistet, die auf dem Knoten *Zertifikate* im I/O-Manager und in der Datenaufzeichnungskonfiguration verfügbar ist. Die folgende Abbildung zeigt den Zertifikatspeicher im I/O-Manager.



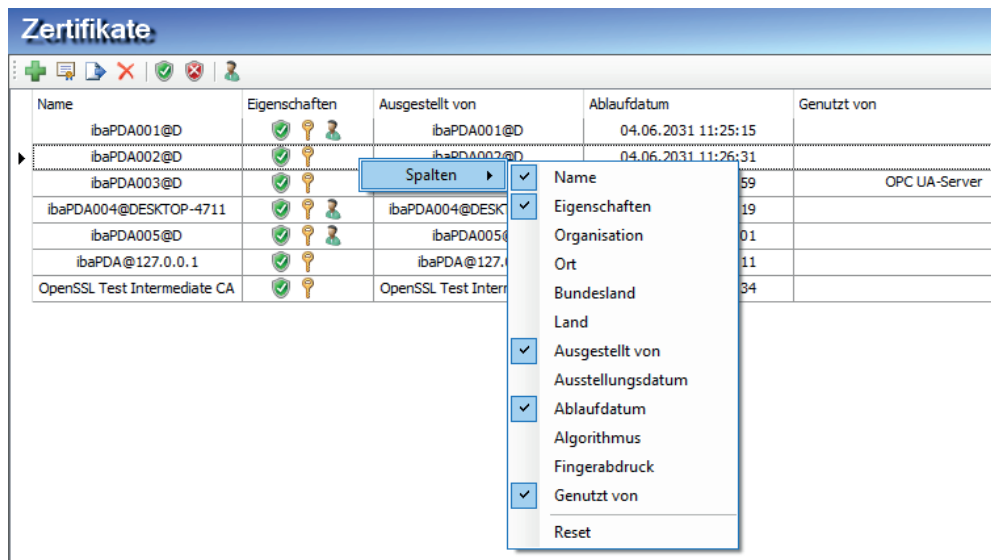
Die folgende Abbildung zeigt den Zertifikatspeicher in der Datenaufzeichnungskonfiguration.



Jede Zeile steht für ein Zertifikat.

Standardmäßig werden die Spalten *Name*, *Eigenschaften*, *Ablaufdatum* und *Genutzt von* angezeigt.

Bei Bedarf können Sie im Kontextmenü der Tabelle weitere Spalten zu- oder abwählen.



In der Spalte *Name* steht der Name des Zertifikats. Dieser ist nicht unbedingt eindeutig, denn mehrere Zertifikate können den gleichen Namen haben. Nur der Fingerabdruck ist einzigartig für ein Zertifikat.

Die Symbole in der Spalte *Eigenschaften* haben folgende Bedeutung:

Symbol	Bedeutung
	Dem Zertifikat wird vertraut, solange es nicht abgelaufen ist.
	Diesem Zertifikat wird nicht vertraut.
	Ein privater Schlüssel für dieses Zertifikat ist verfügbar.
	Dieses Zertifikat kann auch zur Benutzerauthentifizierung genutzt werden.

Tab. 3: Symbole für Zertifikatseigenschaften

In der Spalte *Genutzt von* wird angezeigt, von welcher Applikation/Funktion das Zertifikat verwendet wird. Im Beispiel in der Abbildung oben wird das Zertifikat *ibaPDA003@D* vom OPC UA-Server in *ibaPDA* genutzt. Das heißt, dass dieses Zertifikat bei der Konfiguration des OPC UA-Servers ausgewählt wurde.








Die Anzeige ist eine Kombination aus dem aktuell geöffneten Manager (I/O- oder Datenaufzeichnung) und dem anderen. Das Feld in der Spalte *Genutzt von* hat dabei eine Link-Funktion. Mit einem Doppelklick auf ein ausgefülltes Feld springen Sie zum entsprechenden Konfigurationsdialog innerhalb des geöffneten Managers. Gehört der Eintrag zum anderen Manager, funktioniert der Link nicht. Im Beispiel oben würde ein Doppelklick auf den Eintrag "OPC UA-Server" direkt den Konfigurationsdialog des OPC UA-Servers öffnen, sofern es aus dem I/O-Manager heraus geschieht. Wenn Sie den Zertifikatspeicher in der Datenaufzeichnungskonfiguration geöffnet hätten, würde der Link zum OPC UA-Server nicht funktionieren.

Umgekehrt würde der Sprung zu einer "MQTT Datenaufzeichnung" nur funktionieren, wenn der Zertifikatspeicher aus der Datenaufzeichnungskonfiguration heraus geöffnet wurde.

4.2.3 Zertifikate verwalten

Der zentrale Zertifikatspeicher dient der Verwaltung der Zertifikate. Hier können Sie Zertifikate hinzufügen, erstellen und löschen.

In der Symbolleiste des Zertifikatspeichers finden Sie eine Reihe von Buttons mit folgenden Funktionen:


Button	Funktion
	Mit diesem Button öffnen Sie einen Dialog, mit dem Sie eine vorhandene Zertifikatsdatei laden können. Es werden verschiedene Dateiformate unterstützt (.der, .cer, .crt, .cert, .pem, .pfx, .p12). Falls Sie ein Zertifikat mit einer unbekannten Dateierweiterung haben, erweitern Sie den Dateifilter auf "*.*" und versuchen Sie die Datei trotzdem zu öffnen. In den meisten Fällen funktioniert es.
	Mit diesem Button öffnen Sie einen Dialog, mit dem Sie ein neues Zertifikat erzeugen können.
	Mit diesem Button können Sie ein Zertifikat in eine Datei exportieren, um diese dann für Windows oder eine andere Applikation, z. B. auf einem OPC UA-Client, zu registrieren. Auch hier werden mehrere Dateiformate unterstützt.
	Mit diesem Button entfernen Sie das markierte Zertifikat aus der Tabelle.
	Mit diesem Button kennzeichnen Sie das markierte Zertifikat als „vertrauenswürdig“.
	Mit diesem Button kennzeichnen Sie das markierte Zertifikat als „nicht vertrauenswürdig“. Das Zertifikat bleibt aber trotzdem in der Tabelle des Zertifikatspeichers. Allerdings stehen Zertifikate, denen nicht vertraut wird, in der Auswahlliste für die Verwendung im entsprechenden Konfigurationsdialog nicht zur Verfügung.
	Mit diesem Button legen Sie fest, ob ein Zertifikat auch zur Benutzerauthentifizierung für OPC UA verwendet werden kann.

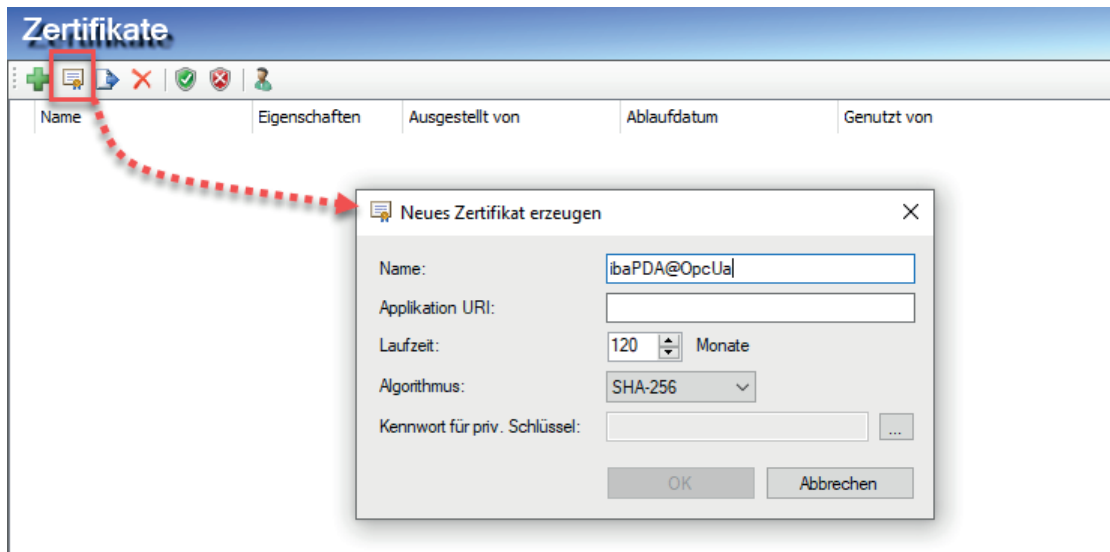
Tab. 4: Buttons in der Symbolleiste für Verwaltung der Zertifikate

Die Befehle beziehen sich stets auf das in der Tabelle ausgewählte Zertifikat, das links am Zeilenanfang mit einem Pfeil gekennzeichnet ist.

4.2.3.1 Ein neues Zertifikat erzeugen

Wenn es noch keine Zertifikate gibt, die Sie laden können, dann müssen Sie eins erzeugen.

1. Klicken Sie auf den Button  und es öffnet sich der folgende Dialog




2. Tragen Sie einen beliebigen Namen für das Zertifikat ein.
3. Tragen Sie bei Bedarf einen Application URI ein.
Der URI (Uniform Resource Identifier) ist eine global eindeutige Identifikation der Applikation, in diesem Fall *ibaPDA*. Wenn Sie dieses Feld nicht ausfüllen, dann wird – sofern vom OPC UA-Client ein Application URI geprüft wird – ein Standard-URI erzeugt, der sich aus Maschinenname und Applikationsname zusammensetzt:
`urn:machinename:applicationName.`
4. Stellen Sie die gewünschte Laufzeit für die Gültigkeit Ihres Zertifikats ein.
5. Wählen Sie den gewünschten Hash-Algorithmus für die Verschlüsselung aus.
SHA-1 ist ein älterer und inzwischen als unsicher eingestufte Hash-Algorithmus, dessen Nutzung nicht mehr empfohlen wird. Manche älteren oder einfacheren OPC UA-Clients unterstützen nur diesen Algorithmus. Zunehmend werden Algorithmen der SHA-2-Familie, also z. B. SHA-256, verwendet, die eine höhere Verschlüsselungstiefe und damit mehr Sicherheit bieten. Aus Sicherheitsgründen sollten Sie diesen bevorzugt wählen, sofern die geplanten Clients ihn auch unterstützen.
6. Geben Sie ein Kennwort, dass Sie selbst festlegen, für den privaten Schlüssel ein. Solange kein Kennwort eingetragen wurde, bleibt der <OK>-Button inaktiv. Um das Kennwort zu vergeben, klicken Sie auf den <...>-Button und tragen Sie das Kennwort zweimal ein und bestätigen Sie mit <OK>. Das Kennwortfeld darf nicht leer bleiben. Es gibt keine besonderen Anforderungen an das Kennwort. Bewahren Sie das Kennwort an einem sicheren Ort auf, damit das selbst erzeugte Zertifikat exportiert und für Windows oder andere Applikationen genutzt werden kann.
7. Schließen Sie den Dialog mit <OK>.

Das neue Zertifikat wird nun in die Liste des Zertifikatspeichers eingetragen und gleich mit den Eigenschaften "vertrauenswürdig" + privater Schlüssel versehen.


Sie können das Zertifikat nun auch exportieren und beim Kommunikationspartner, z. B. einem OPC UA-Client registrieren. Anschließend kann sich der Client dann mit *ibaPDA* (OPC UA-Server) verbinden.

4.2.3.2 Zertifikat hinzufügen

1. Klicken Sie in der Symbolleiste des Zertifikatspeichers auf den Button .
Es öffnet sich ein Dialog, in dem Sie zur gewünschten Zertifikatsdatei navigieren und diese öffnen können.
Es werden verschiedene Dateiformate unterstützt (.der, .cer, .crt, .cert, .pem, .pfx, .p12).
Falls Sie ein Zertifikat mit einer unbekannten Dateierweiterung haben, erweitern Sie den Dateifilter auf "*.*" und versuchen Sie die Datei trotzdem zu öffnen. In den meisten Fällen funktioniert es.
2. Wenn das Zertifikat geladen wurde, erscheint es in der Liste des Zertifikatspeichers.
3. Falls noch nicht geschehen, vertrauen Sie dem Zertifikat.

Zertifikate können mitunter auch ohne einen manuellen Import hinzugefügt werden.


So wird beim ersten Verbindungsversuch eines OPC UA-Clients zum OPC UA-Server (*ibaPDA*) das Anwendungszertifikat des OPC UA-Clients automatisch dem Zertifikatsbereich hinzugefügt und zunächst abgelehnt.

Nachdem Sie das OPC UA-Client-Zertifikat in der Liste markiert und mit dem -Button als vertrauenswürdig eingestuft haben, kann sich der OPC UA-Client im Folgenden automatisch verbinden.

Mithilfe des -Buttons können Sie ein Zertifikat jederzeit wieder ablehnen, bzw. als nicht vertrauenswürdig einstufen.

4.2.3.3 Zertifikate exportieren

Sowohl Zertifikate, die mit *ibaPDA* erzeugt wurden, als auch andere Zertifikate im Zertifikatspeicher können einzeln als Datei exportiert und dann für Windows oder andere Applikationen genutzt werden. Ein exportiertes Zertifikat kann auch wieder in *ibaPDA* reimportiert werden.

Für den Export markieren Sie zuerst das gewünschte Zertifikat in der Tabelle und klicken dann auf den Button  in der Symbolleiste des Zertifikatspeichers.

Wenn Sie ein Zertifikat ohne privaten Schlüssel exportieren wollen, öffnet sich umgehend ein Dialog zum Speichern der Datei.

Wenn das zu exportierende Zertifikat einen privaten Schlüssel hat, gibt es einige Optionen.

Zunächst werden Sie gefragt, ob der vorhandene private Schlüssel mit exportiert werden soll. Wenn sie das verneinen erfolgt sofort die Speicherung, wie bei einem Zertifikat ohne Schlüssel.

Wenn Sie die Frage bejahen, dann müssen Sie anschließend das korrekte Kennwort eingeben. Das korrekte Kennwort ist das Kennwort, das beim Import oder bei der Erzeugung des Zertifikats verwendet wurde. Wenn das Kennwort korrekt ist, kann das Zertifikat als .pfx-Datei gespeichert werden. Diese Datei ist kennwortgeschützt und enthält das Zertifikat und den privaten Schlüssel.

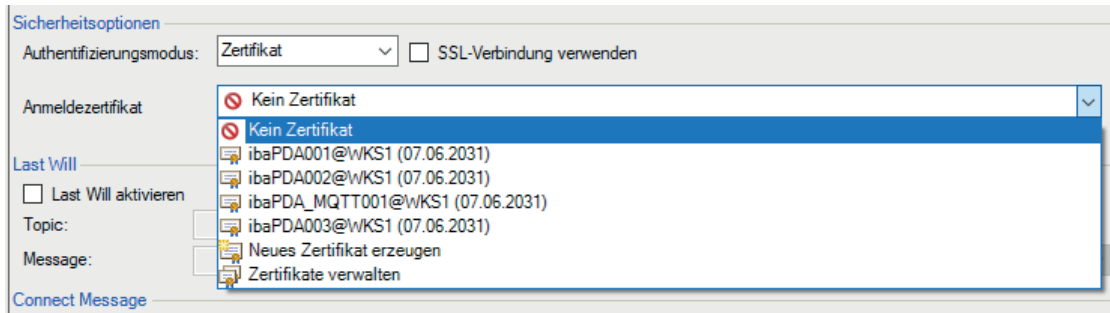
Sollte das Kennwort falsch sein, wird das Zertifikat nicht exportiert.

Unter bestimmten Umständen kann es sein, dass ein Zertifikat mit privatem Schlüssel in *ibaPDA* gespeichert, aber der Schlüssel nicht mit einem Kennwort geschützt ist. In diesem Fall kann das Zertifikat nur ohne privaten Schlüssel exportiert werden. Sie werden dann darauf hingewiesen.

4.2.4 Zertifikate verwenden

An den Stellen, wo Zertifikate zur Anwendung kommen, finden Sie eine Drop-down-Liste, in der die verfügbaren Zertifikate zur Auswahl angeboten werden.

Bei einer MQTT-Datenaufzeichnung sieht das z. B. wie folgt aus:



- **Kein Zertifikat:** Es wird kein Zertifikat benutzt. In der Regel führt das zu einer ungültigen Konfiguration.
- **Verfügbare Zertifikate:** Angezeigt werden alle Zertifikate, die im zentralen Zertifikatspeicher enthalten, gültig und für die Anwendung an dieser Stelle geeignet sind.
- **Neues Zertifikat erzeugen:** Es öffnet sich der Dialog zum Erzeugen eines Zertifikats. Wenn die Erzeugung erfolgreich ist, wird das neue Zertifikat auch gleich ausgewählt. Falls nicht, wird "Kein Zertifikat" eingestellt.
- **Zertifikate verwalten:** Aufruf des zentralen Zertifikatspeichers entweder im I/O-Manager oder in der Datenaufzeichnungskonfiguration, je nachdem wo Sie sich befinden.

Hinweis



Die Auswahl des Zertifikats wird in der Registrierungsdatei des Rechners gespeichert, auf dem der ibaPDA-Client läuft. Im Fall einer neuen Konfiguration wird das gleiche Zertifikat ausgewählt, sofern kein anderes Zertifikat aktiv gewählt wurde.

Andere Dokumentation



Weitere Informationen zu Anwendung und Funktion der Zertifikate finden Sie in den Beschreibungen der betreffenden Schnittstellen, Module und Datenaufzeichnungen.

4.2.5 Speichern und Schützen von Zertifikaten

Die Zertifikate werden in der Datei `settings.xml` gespeichert, die im Programmverzeichnis von *ibaPDA*, Unterordner `Server\Certificates`, liegt. Diese Datei wird automatisch verschlüsselt.

Für die Verwendung von Zertifikaten mit privatem Schlüssel gibt es eine Reihe von Maßnahmen, um Ihre Identität oder die Identität Ihrer Organisation zu schützen. Konkret sind dies Maßnahmen, um den einfachen Export und die Weiterverwendung in Windows oder anderen Applikationen zu erschweren.

- Zertifikate werden stets in verschlüsselter Form gespeichert.
- Für Zertifikate mit privatem Schlüssel ist die Eingabe eines Kennworts erforderlich, ...
 - wenn ein neues Zertifikat erzeugt wird
 - wenn ein Zertifikat mit privatem Schlüssel exportiert wird
 - wenn ein Zertifikat mit privatem Schlüssel importiert wird
- Zertifikate mit privatem Schlüssel können nur exportiert werden, wenn es für den Schlüssel auch ein Kennwort gibt. Gibt es kein Kennwort oder ist das Kennwort unbekannt, kann das Zertifikat nicht mehr exportiert werden. Bewahren Sie daher die Kennwörter an einem sicheren Ort auf.
- Das Kennwort eines privaten Schlüssels kann mit *ibaPDA* nicht geändert werden.
- Für die Nutzung eines Zertifikats in *ibaPDA* ist keine Kennworteingabe erforderlich. Die Datei `settings.xml` kann von einer *ibaPDA*-Installation zu einer anderen kopiert werden, um die Zertifikate dorthin zu übertragen. Auch dafür ist keine Kennworteingabe nötig.

Falls der private Schlüssel in die falschen Hände gerät sind viele Formen des Missbrauchs denkbar. Daher achten Sie auf die sichere Verwahrung der Kennwörter.

4.3 OPC UA Server – Tags

In diesem Register sehen Sie die Tags, die vom OPC UA-Server veröffentlicht werden können. Einige davon sind immer verfügbar, auch wenn Sie die Lizenz *ibaPDA-OPC-UA-Server+* nicht besitzen. Diese Tags haben daher kein Auswahlfeld:

- Name der Software und die Version
- Dongle-spezifische Informationen im Ordner *Licensing*
- Statusinformationen zur Erfassung, z. B. ob die Erfassung läuft oder ob deaktivierte Signale vorhanden sind (*Acquisition*)
- Informationen zu den verbundenen *ibaPDA*-Clients (*Clients*)
- Informationen zu jeder konfigurierten Datenaufzeichnung, geordnet nach Typen (*Data stores*)

Zusätzlich zu diesen standardmäßig verfügbaren OPC UA-Tags können Sie eigene Tags publizieren, wenn Sie die Lizenz *ibaPDA-OPC-UA-Server+* besitzen. Zur Verfügung stehen alle im *ibaPDA*-System konfigurierten Signale. Indem Sie in die Auswahlkästchen vor den Signalen oder vor den Modulen ein Häkchen setzen, werden diese Signale auch als OPC UA-Tags publiziert.

Außerdem können Sie mit der Lizenz *ibaPDA-OPC-UA-Server+* sog. Writable Tags anlegen.

Alle Signale publizieren

Wenn Sie diese Einstellung aktivieren, werden automatisch immer alle in *ibaPDA* existierenden Signale bzw. Tags publiziert. Das bedeutet, auch wenn neue Signale angelegt wurden, werden diese automatisch beim Anwenden der Konfiguration publiziert. Ein manuelles Aktivieren der neuen Signale ist nicht mehr nötig.

Hinweis



Die Tags im OPC UA-Server werden standardmäßig wie die Ausgänge von *ibaPDA* aktualisiert. Der schnellste Aktualisierungszyklus ergibt sich also aus dem kleinsten gemeinsamen Vielfachen aller Modulzeitbasen, bzw. beträgt mindestens 50 ms. Nur wenn im Register *Konfiguration* die Option für ein abweichendes Mindestpublikationsintervall aktiviert ist, kann ein langsamerer Aktualisierungszyklus eingestellt werden.

Tag-Beschreibung

Diese Beschreibung erscheint bei einem OPC UA Client, der sich mit dem Server verbindet, beim Browsen der Tags. Ein Tag kann damit näher beschrieben werden. Der Anwender kann wählen, ob die Felder "Kommentar 1", "Kommentar 2" oder die Kombination aus beiden "Kommentar 1 | Kommentar 2" dafür verwendet werden.

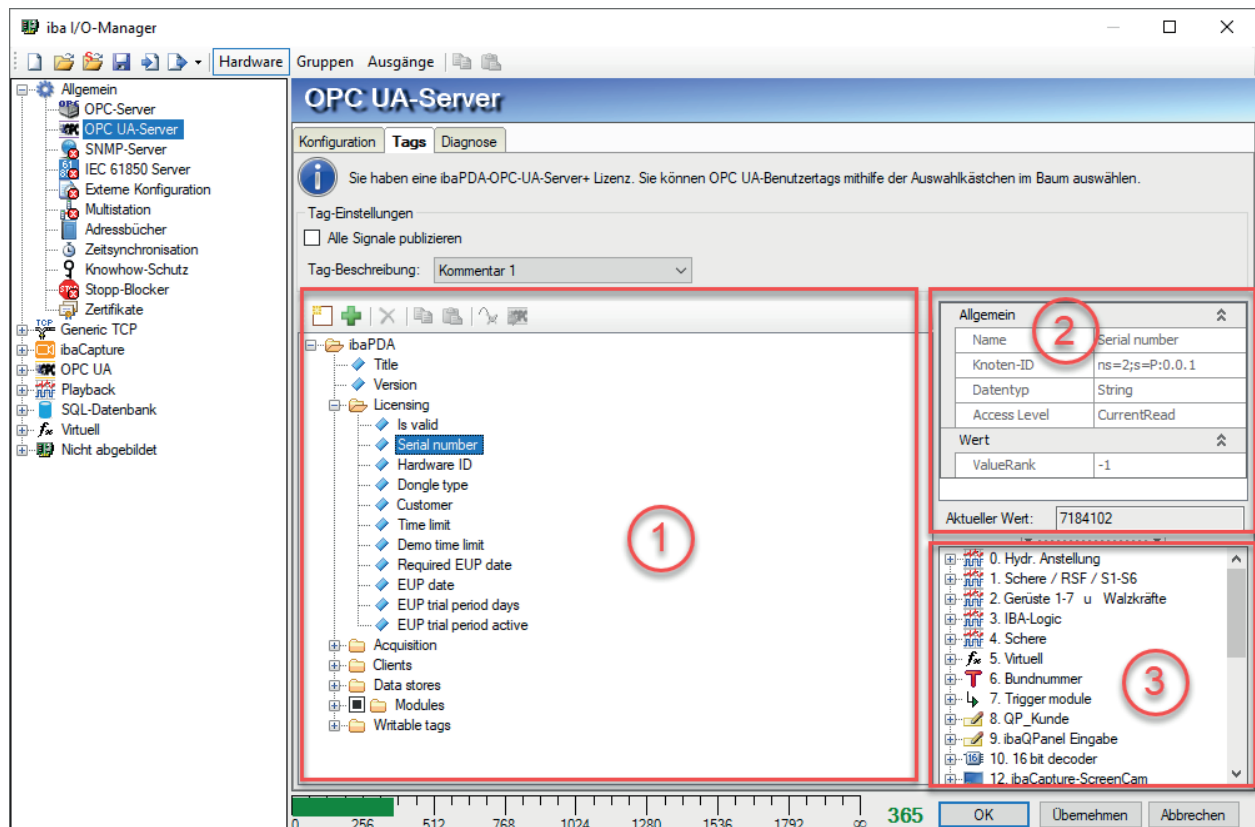
Tag-Verzeichnis und Info-Bereich

Das Tag-Verzeichnis zeigt alle verfügbaren Tags in einer Baumstruktur.

Hier können Sie folgende Handlungen vornehmen:

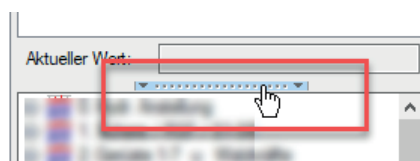
- Markieren der erfassten Messsignale, um diese zu publizieren
- Hinzufügen von Writable Tags
- Hinzufügen von benutzerdefinierten Informationsmodellen

Rechts daneben befindet sich der Info-Bereich. Markieren Sie einen Tag im Verzeichnis, dann werden im Info-Bereich sein Istwert und weitere Informationen wie z. B. Name, Knoten-ID und Datentyp angezeigt.










- 1 Tag-Verzeichnis mit Standard-Tags, erfassten Signalen und Writable Tags sowie Informationsmodellen
- 2 Info-Bereich mit Angabe von Tag-Name, Knoten-ID, Datentyp und Access Level sowie aktuellem Wert
- 3 Signalbaumfenster für die Zuweisung von erfassten Signalen zu den Tags eines benutzerdefinierten Informationsmodells

Klicken Sie auf die schmale Schallfläche auf dem Fensterrahmen, um das Fenster anzuzeigen oder zu verbergen.



Über dem Tag-Verzeichnis befindet sich eine Symbolleiste mit folgenden Funktionen:

	Eine neue Konfiguration erzeugen	Alle konfigurierten Signale und importierten Tags werden entfernt. ibaPDA-Standardtags bleiben erhalten.
	OPC UA Node-Set hinzufügen	Öffnet den Dialog zum Importieren einer Node-Set-Datei (*.xml).
	Gewähltes Tag oder Element entfernen	Nur verfügbar für Writable Tags-Ordner, Writable Tags und Node-Set
	Gewähltes Element in die Zwischenablage kopieren	Nur verfügbar, wenn ein kopierfähiges Element markiert ist (Writable Tag oder Writable Tag-Ordner)
	Inhalt der Zwischenablage einfügen	Ist nur verfügbar, wenn ein Ordner markiert ist, in den das Element aus der Zwischenablage eingefügt werden kann. Ein kopierter Writable Tag kann z. B. nur in einen Ordner <i>Analog</i> oder <i>Digital</i> eingefügt werden.
	Signalverbindung zu den Tags in einem Node-Set lösen	Nur verfügbar, wenn mindestens ein Node-Set vorhanden ist und der Root-Ordner des Node-Sets, ein Unterordner innerhalb des Informationsmodells oder ein Tag markiert ist. Ein oder mehrere Tags markiert: Signalverbindung dieser Tags wird gelöst; Ordner markiert: Die Signalverbindungen aller Tags in diesem Ordner werden gelöst; Root Node-Set markiert: Alle Signalverbindungen zu Tags in diesem Node-Set werden gelöst;
	OPC-UA Server-Modul zuweisen	Ist nur verfügbar, wenn ein Writable Tags-Ordner markiert ist. Mausklick auf diese Symboltaste erzeugt im I/O-Manager unter der Schnittstelle OPC UA ein OPC UA Server-Modul mit dem Namen des Ordners. Alle in dem Ordner enthaltenen Tags werden in die Signaltabellen <i>Analog</i> und <i>Digital</i> des Moduls übernommen, mit Name, Knoten-ID und Datentyp.

4.3.1 Standard-Tags

Licensing

Diese Tags geben Auskunft über den Dongle, die Lizenznummer (Seriennummer) und Demo- bzw. EUP-Daten.

Acquisition

Diese Tags geben Auskunft darüber, ob die Erfassung läuft, ob es deaktivierte Signale gibt, was der Grund für den letzten Start der Erfassung war und wie lange die Erfassung seit dem letzten Start läuft (in Sekunden).

Enumeration	Beschreibung	Werte
IbaEnumPDASStartReason	Die möglichen Gründe für den Start der Datenerfassung	0...keiner (none) 1...Start-Button (startButton) 2... neue I/O-Konfiguration (newIOConfig) 10...automatischer Start (automaticStart) 11. Remote Konfiguration (remoteConfig)

Tab. 5: Enumerations für Startgrund der Erfassung

Clients

Diese Tags geben Auskunft darüber, wie viele und welche *ibaPDA*-Clients mit dem *ibaPDA*-Server verbunden sind. Weitere Informationen wie angemeldeter Benutzer, IP-Adresse, Zeitpunkt als der Client sich verbunden hat und Anzahl der aktuell angeforderten Signale werden zur Verfügung gestellt. Bei mehreren Clients werden die entsprechenden Werte durch Kommata getrennt. Die Anzahl der Werte richtet sich nach der Anzahl der Client-Lizenzen.

Data Stores

Diese Tags geben Auskunft darüber, welche Datenaufzeichnungen definiert sind und welchen Status sie haben. Für jede Art der Datenaufzeichnung gibt es einen separaten Zweig. Wenn mehrere Datenaufzeichnungen eines Typs definiert sind, werden die entsprechenden aktuellen Werte durch Kommata getrennt.

Enumeration	Beschreibung	Werte
IbaEnumDBTimeStoreStatus	Die möglichen Zustände einer DB/Cloud Datenaufzeichnung	0...angehalten (stopped) 1...warten auf Trigger (waitForTrigger) 2...Aufzeichnung (recording) 3...Post-Trigger (stopCountDown)
IbaEnumPDASToreStatus	Die möglichen Zustände einer ibaPDA-Datenaufzeichnung	0...angehalten (stopped) 1...warten auf Trigger (waitForTrigger) 2...Aufzeichnung (recording) 3...Post-Trigger (stopCountDown)
IbaEnumQDRStoreStatus	Die möglichen Zustände einer iba-QDR-Datenaufzeichnung	0...angehalten (stopped) 1...nicht synchron (unsynched) 2...synchron (syncd)
IbaEnumHDStoreStatus	Die möglichen Zustände einer iba-HD-Datenaufzeichnung	0...angehalten (stopped) 1...getrennt (disconnected) 2...Aufzeichnung (recording)

Tab. 6: Enumerations für Statuswerte der Aufzeichnungsarten

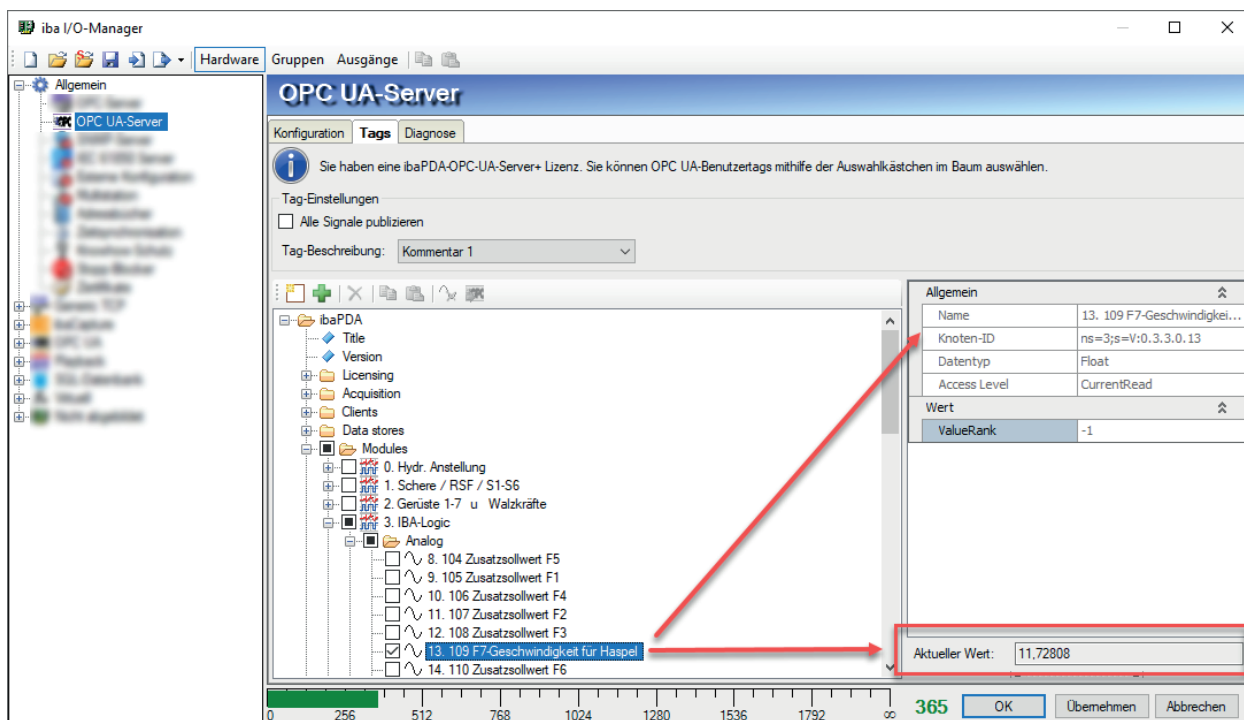
4.3.2 Erfasste Signale (Modules)

Alle in *ibaPDA* konfigurierten Signale, also Analog-, Digital- und Textsignale, Eingangs-, Ausgangs- und virtuelle Signale können über den OPC UA-Server publiziert werden.

Im Ordner *Modules* des Tag-Verzeichnisses sind alle Module mit ihren Signalen in Form des Signalbaums zu finden.

Um Signale zu publizieren, müssen Sie die gewünschten Signale oder Module mit einem Häkchen markieren.

Wenn Sie einen Signal-Tag anklicken, werden im Info-Bereich wieder die Daten zum Tag angezeigt. Der aktuelle Wert des Signals wird nur angezeigt, wenn die Erfassung läuft.



4.3.3 Writable Tags

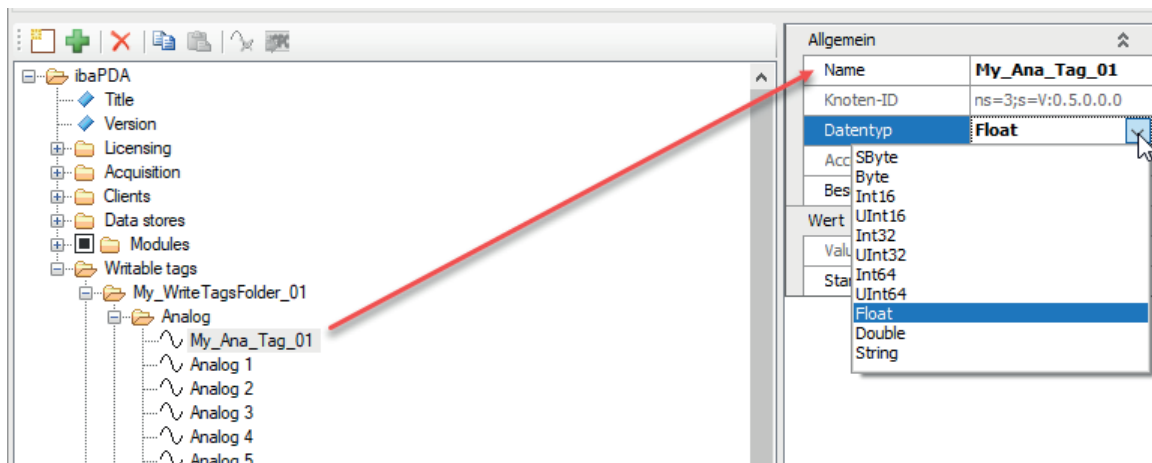
Writable Tags sind Tags, die auf dem OPC UA-Server definiert sind, aber von OPC UA-Clients gelesen und beschrieben werden können.

Konfiguration

Sie können beliebig viele Ordner mit Writable Tags anlegen. Erweitern Sie dazu den Knoten *Writable Tags* und klicken Sie auf *Neuen beschreibbaren Tag-Ordner hinzufügen*. Es wird ein neuer Ordner mit standardmäßig 32 Analog- und 32 Digitalsignalen angelegt.

Markieren Sie den Ordner und geben Sie ihm im Info-Bereich, Feld *Name*, einen passenden Namen.

Auch die beschreibbaren Tags können Sie hier konfigurieren, indem Sie ihnen Namen geben, einen Datentypen zuordnen und ggf. einen Standardwert vorgeben.



Sie können außerdem weitere Tags einzeln hinzufügen und - mit rechtem Mausklick - kopieren oder löschen. Um einen kopierten Tag einzufügen, klicken Sie mit der rechten Maustaste auf das gewünschte Ordnersymbol und wählen dann *Einfügen*.

Tipp



Es ist sinnvoll, die Tags hier schon vollständig mit aussagekräftigen Namen, Datentyp und ggf. Standardwert zu konfigurieren. Wenn von Client-Seite auf den OPC UA Server zugegriffen wird, erscheinen die Tags in lesbarer, verständlicher Form.

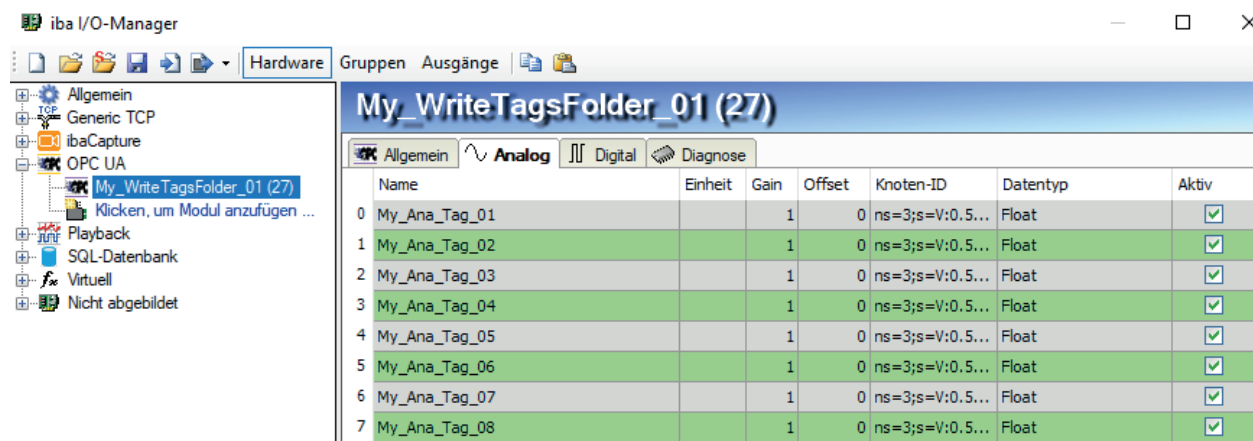
Writable Tags als Signale in ibaPDA anzeigen und aufzeichnen

Sowie die beschreibbaren Tags definiert wurden, stehen sie auf OPC UA-Ebene zur Verfügung. Damit diese Tags bzw. ihre Werte aber in *ibaPDA* angezeigt und/oder aufgezeichnet werden können, müssen sie einem OPC UA-Server-Modul zugewiesen werden.

Das geht sehr einfach, indem Sie mit der rechten Maustaste auf den Ordner klicken und im Kontextmenü *OPC UA Server-Modul zuweisen* wählen. Alternativ können Sie die entsprechende Symboltaste anklicken.

Unter der OPC UA-Schnittstelle im I/O-Manager wird ein entsprechendes Modul angelegt, das den Namen des Ordners trägt. Auch für alle enthaltenen Tags werden automatisch entsprechen-

de Signale im Modul angelegt. Name, Knoten-ID und Datentyp werden wie zuvor im OPC UA Server konfiguriert übernommen.



Sie können bei Bedarf die Signalnamen anschließend in den Signaltabellen des OPC UA Server-Moduls ändern. Das hat keine Rückwirkung auf die Namen der Tags.

Sie können darüber hinaus das OPC UA Server-Modul umkonfigurieren, indem Sie Signale herauslöschten oder über den OPC UA Symbolbrowser ganz andere Tags mit dem Modul verbinden.

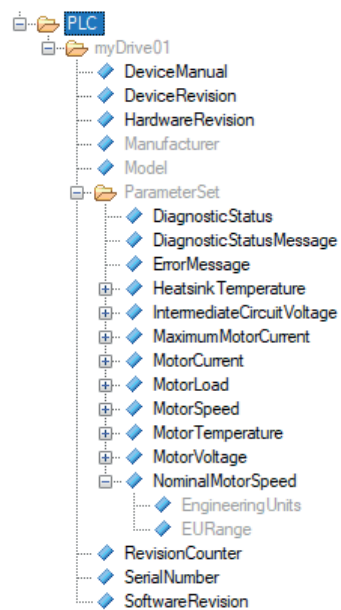
4.3.4 Benutzerdefinierte Informationsmodelle

ibaPDA-OPC UA-Server unterstützt den Import von sogenannten UA Node-Sets. Nach dem Import können den Tags in diesem Node-Set Signale aus dem *ibaPDA*-Signalbaum zugeordnet werden.

Einleitung

UA Node-Sets bilden bestimmte Informationsmodelle ab, die für die Standardisierung von Kommunikationsschnittstellen sehr hilfreich sind. Bei einem UA Node-Set handelt es sich um eine strukturierte Zusammenstellung relevanter Tags, die für eine bestimmte Anwendung, z. B. bei einer Maschine, ausgelegt ist.

Die folgende Abbildung zeigt ein Beispiel für ein Informationsmodell zu einem Antrieb, dessen Gerätedaten, Statusinformationen und Parameter mit einer SPS ausgetauscht werden sollen.



Für die Erzeugung solcher UA Node-Sets gibt es spezielle Modellierungswerkzeuge wie z. B. Siemens OPC UA Modeling Editor (SiOME) oder Unified Automation UaModeler. Unter Anwendung sogenannter Companion Specifications werden damit Informationsmodelle erstellt und als XML-Datei (Node-Set-Datei) ausgeleitet. Diese Datei kann in ibaPDA importiert werden.

Die folgende Abbildung zeigt beispielhaft den Header einer Node-Set-Datei.



Importieren und Entfernen eines UA Node-Sets

1. Klicken Sie in der Symbolleiste über dem Tag-Verzeichnis auf das grüne Kreuz.
2. Wählen Sie die gewünschte Node-Set-Datei (*.xml) aus und klicken Sie auf <Öffnen>.
3. Das komplette Node-Set wird als neuer Hauptzweig in das Tag-Verzeichnis unter dem ibaPDA-Rootzweig gehängt, wie in dem Bild oben "PLC".

Mit jedem Import wird wieder ein neues Node-Set hinzugefügt. Wenn mehrere gleichartige Objekte, wie z. B. gleiche Antriebe, abgebildet werden sollen, müssen Sie den Import mehrfach ausführen.

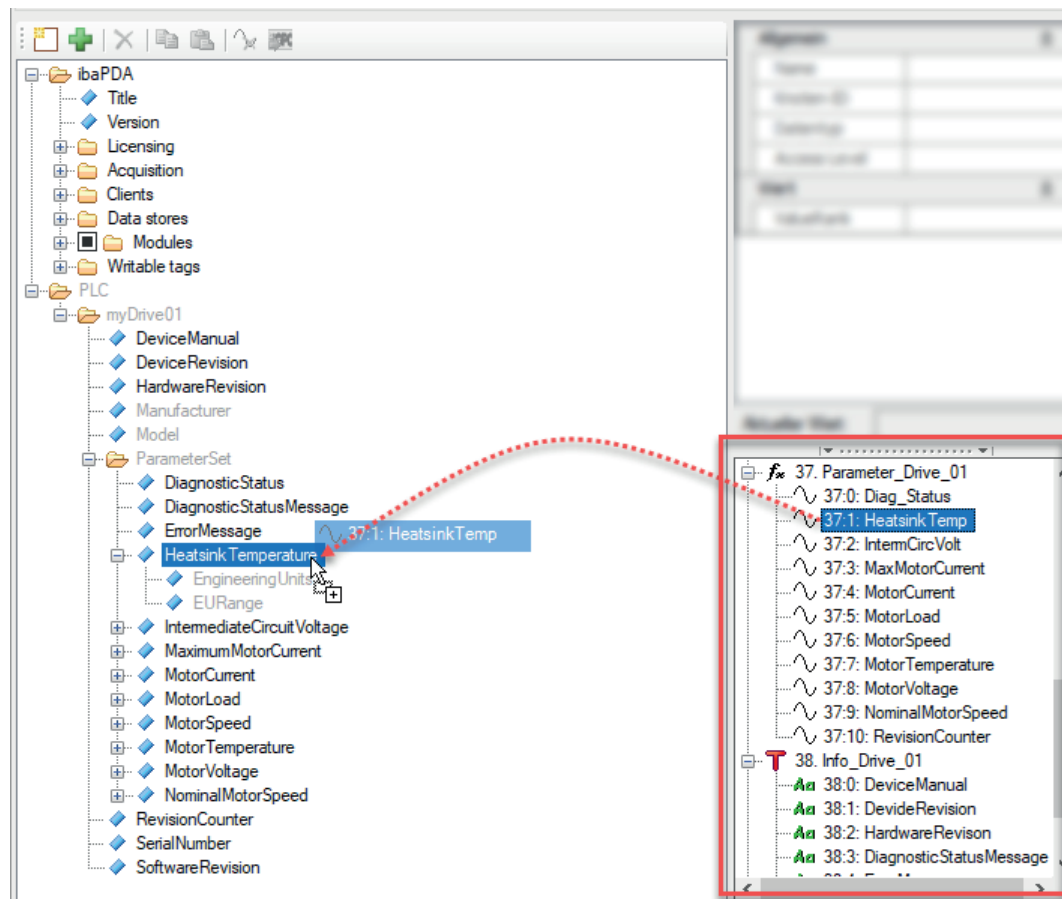
Sowie mindestens ein Node-Set vorhanden ist, sind die Symboltasten zum Entfernen von Node-Sets und zum Lösen der Verbindung zu einem Signal verfügbar.

Wenn Sie ein Node-Set wieder entfernen wollen, markieren Sie den Hauptknoten des betreffenden Node-Sets und klicken Sie auf das rote X.

ibaPDA-Signale mit dem Node-Set verbinden

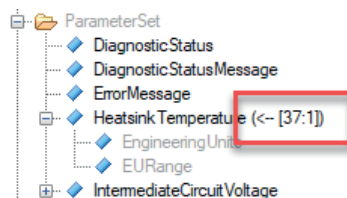
Importierte Tags, die nicht mit Signalen verknüpft werden können, werden grau dargestellt. Das sind z. B. Ordner oder Tags mit Datentypen, die nicht unterstützt werden.

Um ein Signal mit einem Tag zu verknüpfen, ziehen Sie einfach per Drag & Drop das gewünschte Signal aus dem Signalbaumfenster auf der rechten Seite auf den passenden Tag im Tag-Verzeichnis auf der linken Seite.



Im Beispiel (Abbildung oben) wird die mit *ibaPDA* gemessene Kühlkörpertemperatur ("HeatsinkTemp") eines Antriebs dem passenden Tag "HeatsinkTemperature" zugewiesen.

Ist eine Verknüpfung vorhanden, wird hinter dem Tag-Namen die Signal-ID (Modulnr.:Signalnr.) angezeigt.



Wollen Sie ein bereits zugewiesenes Signal durch ein anderes ersetzen, ziehen Sie einfach das neue Signal auf den Tag.

Sie können eine Signalverknüpfung jederzeit wieder lösen, indem Sie den Tag markieren und auf die Symboltaste für *Signalverbindungen entfernen* klicken.

5 Diagnose

5.1 Lizenz

Falls Sie die konfigurierten Signale nicht als OPC UA-Variablen veröffentlichen können, überprüfen Sie entweder in *ibaPDA* im I/O-Manager unter *Allgemein - Einstellungen - Lizenz-Info* oder in der *ibaPDA*-Dienststatus-Applikation, ob Ihre Lizenz „ibaPDA OPC-UA Server+“ ordnungsgemäß erkannt wird.

Lizenz-Info

Lizenz-Nr. :

Kunde:

Nutzungsdauer:

Dongle HW ID:

Daten-Aufzeichnungen:

Lizenz-Optionen:

- ibaPDA OPC-UA Server+

Sollte keine Lizenz vorhanden sein, werden Sie außerdem im I/O-Manger, Zweig *Allgemein - OPC UA-Server*, Register *Variablen*, darauf hingewiesen:

Konfiguration **Tags** Diagnose

Sie haben keine ibaPDA-OPC-UA-Server+ Lizenz. Es ist Ihnen nicht gestattet, OPC UA Benutzer-Tags auszuwählen. Nur die Tags ohne Auswahlkästchen im Baum sind im OPC UA Server verfügbar.

5.2 Register Diagnose

Im Register *Diagnose* (I/O-Manager, Zweig *Allgemein - OPC UA-Server*) wird der aktuelle Status des OPC UA-Servers angezeigt. Außerdem sehen Sie dort eine Liste der verbundenen OPC UA-Clients und Abonnements.

The screenshot shows the 'Diagnose' tab with the following information:

Status: **OPC UA server running**

Verbundene OPC UA Clients

Name	ID	Letztes Telegramm
ibaPDA [OPC UA Client]	ns=4;i=1966665814	11:08:36
urn:DEVPC-HARRISON:UnifiedAutomation:U...	ns=4;i=1966665902	11:08:35

Abonnements

ID	Anzahl überwachter Elem...	Publishing-Interval	Nächste Sequenznummer
3	2	50 ms	949
4	1	100 ms	1

Für jede Verbindung werden Name und ID der Sitzung zusammen mit dem jüngsten Zeitstempel, an dem Kommunikation stattgefunden hat, angezeigt.

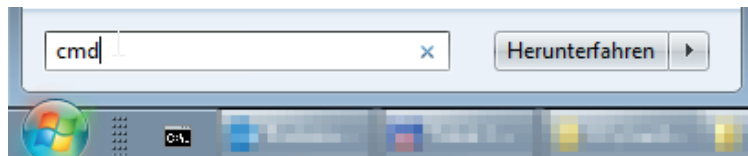
Für jedes Abonnement werden die Abonnement-ID, die Anzahl der beobachteten Variablen, das Publikationsintervall und die nächste Sequenznummer angezeigt. Letzterer Wert wird jedes Mal erhöht, wenn neue Daten für ein bestimmtes Abonnement gesendet wurden.

Wenn Sie in der oberen Liste einen OPC UA-Client anwählen, dann werden die Abonnements gefiltert, so dass in der unteren Liste nur die für diesen Client relevanten Abonnements angezeigt werden.

5.3 Verbindungsdiagnose mittels PING

Ping ist ein System-Befehl, mit dem überprüft werden kann, ob ein bestimmter Kommunikationspartner in einem IP-Netzwerk erreichbar ist.

Öffnen Sie eine Windows Eingabeaufforderung.



Geben Sie den Befehl „ping“ gefolgt von der IP-Adresse des Kommunikationspartners ein und drücken Sie <ENTER>.

Bei bestehender Verbindung erhalten Sie mehrere Antworten.

A screenshot of a Windows command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The window shows the output of a successful ping command. The text is as follows:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>ping 192.168.1.10

Ping wird ausgeführt für 192.168.1.10 mit 32 Bytes Daten:
Antwort von 192.168.1.10: Bytes=32 Zeit=1ms TTL=30
Antwort von 192.168.1.10: Bytes=32 Zeit<1ms TTL=30
Antwort von 192.168.1.10: Bytes=32 Zeit<1ms TTL=30
Antwort von 192.168.1.10: Bytes=32 Zeit<1ms TTL=30

Ping-Statistik für 192.168.1.10:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

C:\Windows\system32>
```

Bei nicht bestehender Verbindung erhalten Sie Fehlermeldungen.

A screenshot of a Windows command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The window shows the output of a failed ping command. The text is as follows:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>ping 192.168.1.10

Ping wird ausgeführt für 192.168.1.10 mit 32 Bytes Daten:
Antwort von 192.168.1.100: Zielhost nicht erreichbar.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.1.10:
    Pakete: Gesendet = 4, Empfangen = 1, Verloren = 3
    (75% Verlust),

C:\Windows\system32>
```

6 Support und Kontakt

Support

Tel.: +49 911 97282-14
Fax: +49 911 97282-33
E-Mail: support@iba-ag.com

Hinweis



Wenn Sie Support benötigen, dann geben Sie bitte bei Softwareprodukten die Lizenznummer bzw. die CodeMeter-Containernummer (WIBU-Dongle) an. Bei Hardwareprodukten halten Sie bitte ggf. die Seriennummer des Geräts bereit.

Kontakt

Hausanschrift

iba AG
Königswarterstraße 44
90762 Fürth
Deutschland

Tel.: +49 911 97282-0
Fax: +49 911 97282-33
E-Mail: iba@iba-ag.com

Postanschrift

iba AG
Postfach 1828
90708 Fürth

Warenanlieferung, Retouren

iba AG
Gebhardtstraße 10
90762 Fürth

Regional und weltweit

Weitere Kontaktadressen unserer regionalen Niederlassungen oder Vertretungen finden Sie auf unserer Webseite

www.iba-ag.com.