Unified-E OPC UA Adapter Benutzerhandbuch

OPC UA-Endpunkte und Datenpunkte konfigurieren

Software-Version 3.1.0.0, zuletzt aktualisiert: Juli 2025

Herausgeber: Unified-E AG, Winterthur, Schweiz

Inhalt

1 Allgemeines 3
1.1 Einführung 3
1.2 Verschlüsselte Kommunikation 3
2 Adapter-Parameter in Unified-E 3
2.1 Endpunkt-Adresse 4
2.2 Adapter-Parameter 4
3 Datenpunkte hinzufügen 5
3.1 Datenpunkte online auswählen 5
3.2 Adressierung von Datenpunkten 6

1 Allgemeines

1.1 Einführung

OPC UA (Open Platform Communications Unified Architecture) ist ein plattformunabhängiges, standardisiertes Protokoll für die industrielle Kommunikation. Es ermöglicht den sicheren und zuverlässigen Austausch von Daten zwischen Maschinen, Steuerungen und Visualisierungen.

Der OPC UA Adapter erlaubt es, Prozessdaten eines OPC UA Servers (z. B. einer Steuerung) in einer Unified-E HMI-Applikation zu verwenden. Hierzu werden Datenpunkte konfiguriert, die über den Adapter gelesen und geschrieben werden können.

Immer mehr SPS-Steuerungs-Hersteller bieten inzwischen standardmässig eine OPC UA-Schnittstelle an (z. B. Codesys-Steuerungen, B&R-Steuerungen).

1.2 Verschlüsselte Kommunikation

OPC UA ermöglicht eine verschlüsselte Kommunikation. Die Kommunikations-Teilnehmer autorisieren sich jeweils mit einem SSL-Zertifikat.

Vom Kommunikations-Partner muss das SSL-Zertifikat als vertrauenswürdig eingestuft werden. Dies kann auf folgende Arten geschehen:

1. Das SSL-Zertifikat wurde auf dem Gateway-PC über Standard-Mechanismen als vertrauenswürdig deklariert oder wurde von einer vertrauenswürdigen Zertifizierungsstelle herausgegeben (nur für erfahrene Administratoren empfohlen)
2. Das SSL-Zertifikat (nur der öffentliche Schlüssel) wird in einen definierten Speicherort kopiert, das alle vertrauenswürdigen Zertifikate enthält

Speicherort der eigenen Client-Zertifikate:

%ProgramData%\OPC Foundation\CertificateStores\MachineDefault\certs

%ProgramData%\OPC Foundation\CertificateStores\MachineDefault\private

Der OPC UA Adapter benutzt diese Zertifikate, um zum Beispiel Datenpakete zu signieren.

Speicherort der vertrauenswürdigen Server-Zertifikate:

%ProgramData%\OPC Foundation\CertificateStores\UA Applications\certs

Kopieren Sie die Zertifikate der vertrauenswürdigen OPC UA Server in dieses Verzeichnis.

2 Adapter-Parameter in Unified-E

Die Endpunkt-Adresse und die Adapter-Parameter können im Unified-E App Designer oder auch im Unified-E App Manager gesetzt werden.

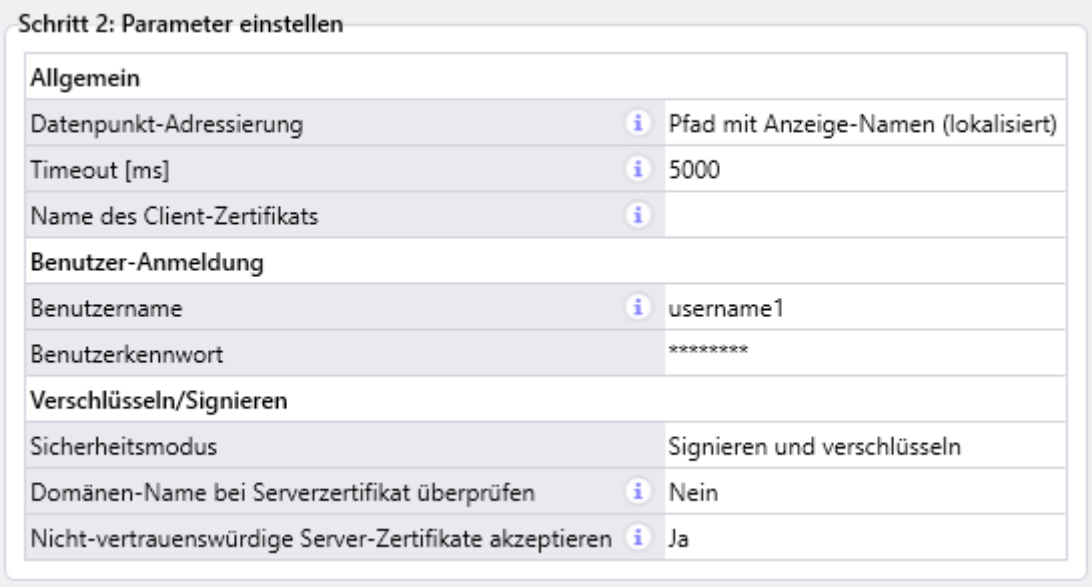
2.1 Endpunkt-Adresse

Die Endpunkt-Adresse identifiziert den OPC UA-Server im Netzwerk eindeutig.

Beispiele für Adressen:

- opc.tcp://192.168.1.20:48020
- opc.tcp://13.250.XXX.XXX:5220/RMS343/DataAccessServer

2.2 Adapter-Parameter



Allgemein:

- Datenpunkt-Adressierung: Legt fest, wie eine OPC-Variable angesprochen wird. Es stehen folgende Optionen zur Verfügung:
    - Pfad mit Anzeige-Namen (lokalisiert): Der Adresspfad besteht aus Segmenten wie «Demo/Static/Scalar/Boolean». Falls mehrere Knoten denselben Namen haben, wird der erste passende Knoten verwendet. Die Segmente sind mehrsprachig
    - Pfad mit Browse-Namen: Der Adresspfad besteht aus Segmenten wie «Demo/Static/Scalar/Boolean». Falls mehrere Knoten denselben Namen haben, wird der erste passende Knoten verwendet. Die Segmente bezeichnen den Browse-Name des Knotens
    - Knoten-ID (schnell): Die Variable wird direkt über die eindeutige NodeI-ID identifiziert, z. B. « ns=4;s=SimulationSpeed». Diese Methode ist am performantesten und wird empfohlen, wenn die Node-ID bekannt ist und sich nicht mehr ändert

- Timeout [ms]: Gibt an, wie lange auf eine Antwort vom Server gewartet wird (z. B. beim Verbindungsaufbau oder Lesen von Werten). Der Wert wird in Millisekunden angegeben.
- Name des Client-Zertifikats: Subject-Name des zu verwendenden Client-Zertifikats.
    - Dieses Zertifikat muss sich im Verzeichnis %ProgramData%\OPC Foundation\CertificateStores\MachineDefault\certs befinden
    - Wenn kein Name angegeben ist, wird automatisch ein temporäres Client-Zertifikat erzeugt

Benutzer-Anmeldung:

- Benutzername / Benutzerkennwort: Optional – falls der OPC UA Server eine Authentifizierung über Benutzername und Passwort verlangt.
    - Das Passwort wird verschlüsselt gespeichert

Verschlüsseln / Signieren:

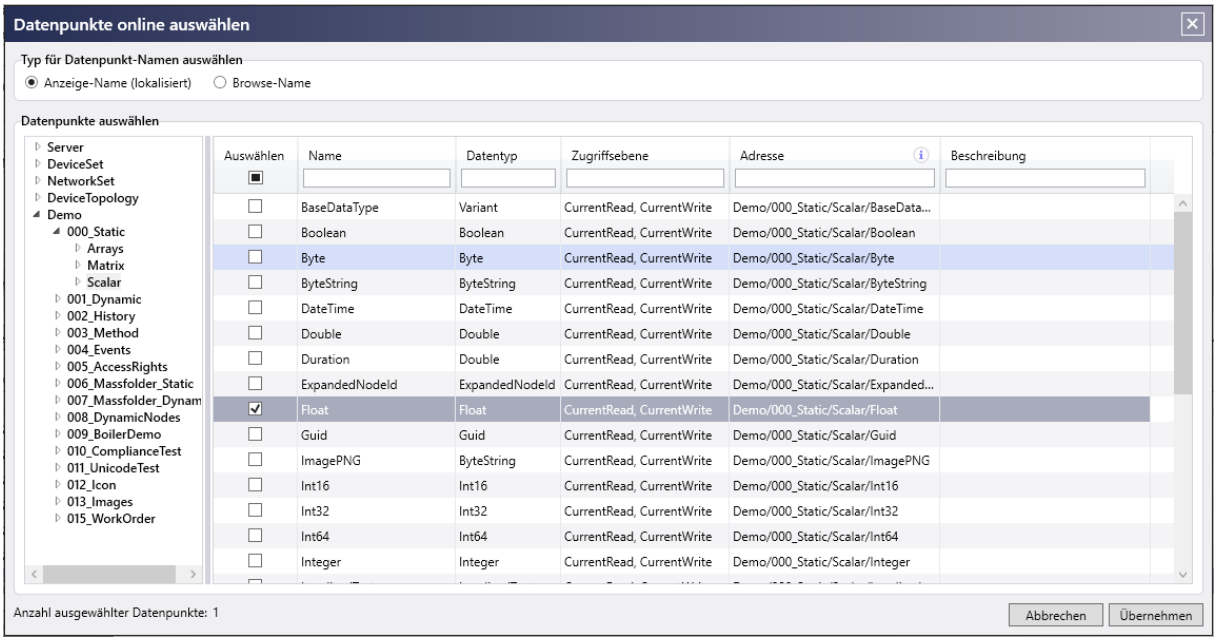
- Sicherheitsmodus: Legt fest, wie die Datenkommunikation abgesichert wird:
    - Keine: Daten werden unverschlüsselt übertragen. Keine weiteren Parameter erforderlich
    - Signieren: Die Daten werden mit dem Client-Zertifikat signiert, aber nicht verschlüsselt
    - Signieren und verschlüsseln: Die Kommunikation wird vollständig abgesichert – sowohl signiert als auch verschlüsselt
- Domänen-Name bei Serverzertifikat überprüfen: Wenn aktiv (Wert «Ja»), wird geprüft, ob der Domänenname im Serverzertifikat mit der tatsächlichen Serveradresse übereinstimmt.
    - Diese Option erhöht die Sicherheit, kann aber bei internen Netzwerken deaktiviert werden.
- Nicht-vertrauenswürdige Server-Zertifikate akzeptieren: Wenn aktiv (Wert «Ja»), werden auch Zertifikate akzeptiert, die nicht durch eine vertrauenswürdige Zertifizierungsstelle signiert wurden.
    - Diese Einstellung wird in Testumgebungen oder bei selbstsignierten Zertifikaten benötigt.

3 Datenpunkte hinzufügen

3.1 Datenpunkte online auswählen

Am einfachsten fügen Sie neue Datenpunkte im Unified-E App Designer im Endpunkte-Editor über die Schaltfläche «Datenpunkte online auswählen» hinzu (siehe App-Designer-Handbuch). Beim Klicken dieser Schaltfläche wird ein Dialog zur Auswahl der gewünschten Datenpunkte des verbundenen OPC UA-Servers geöffnet. Die ausgewählten Datenpunkte werden automatisch in die Datenpunkte-Tabelle übernommen. Eine manuelle Eingabe der

Datenpunkt-Adresse ist dabei nicht erforderlich – die Adresse wird automatisch gemäss dem Parameter «Datenpunkt-Adressierung» (siehe oben) eingetragen.



3.2 Adressierung von Datenpunkten

Die Adresse eines Datenpunktes ist abhängig von der gewählten Adressierungsart, die durch den Parameter «Datenpunkt-Adressierung» bestimmt wird – siehe oben.

Im Folgenden werden die unterschiedlichen Datenpunkt-Adressierungen genauer beleuchtet.

Datenpunkt-Adressierung: «Pfad mit Browse-Namen»:

- Vorteil: Die Adresse ist gut lesbar, z. B. «Demo/000_Static/Scalar/Byte».
- Nachteil: Initial beim Verbindungsaufbau muss immer zuerst die Knoten-ID vom Browse-Namen-Pfad ermittelt werden – was eine Kommunikation mit den OPC UA-Server erfordert und bei vielen Datenpunkten und langsamer Verbindung zu Performance-Problemen führen kann.

Datenpunkt-Adressierung: «Node-ID (schnell)»:

- Vorteil: Schnelle Verbindung, der Browse-Pfad muss nicht aufgelöst werden, da die Knoten-ID, welche für die Kommunikation notwendig ist, bereits vorliegt.
- Nachteil: Die Knoten-ID ist je nach OPC UA-Server weniger gut lesbar und könnte sich bereits ändern, wenn im OPC UA-Server neue Variablen hinzugefügt werden oder sich das SPS-Programm ändert.

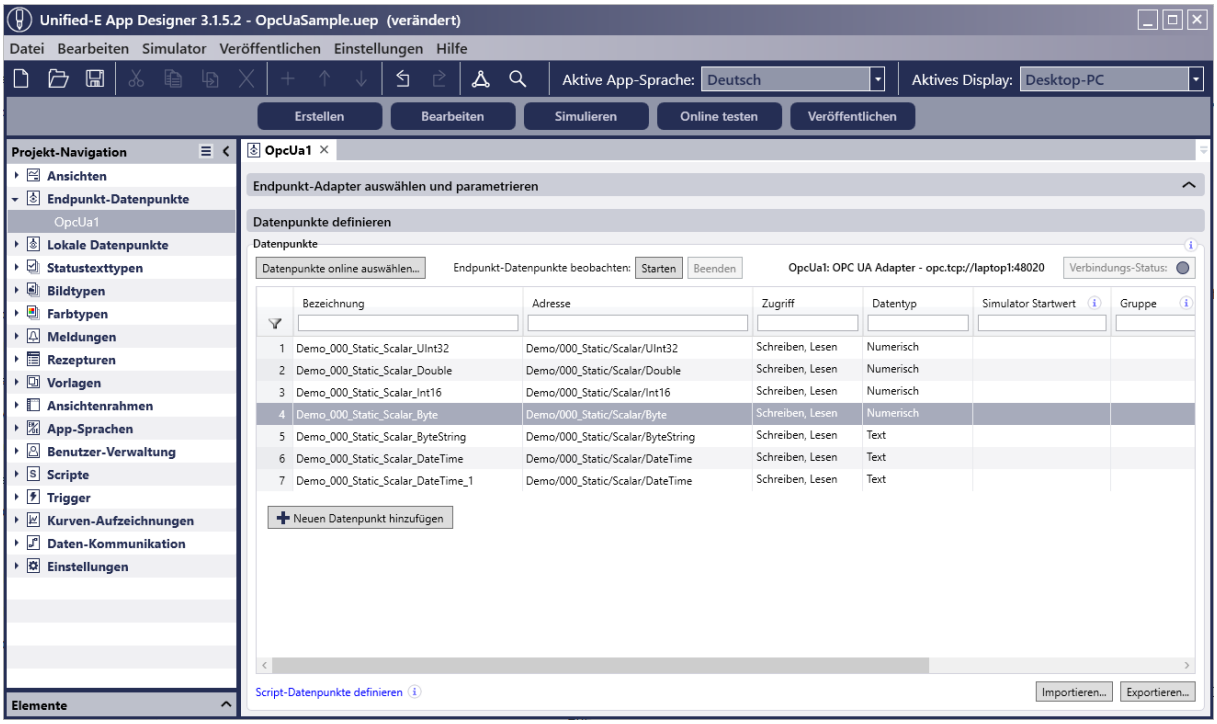
Datenpunkt-Adressierung: «Pfad mit Anzeige-Namen (lokalisiert)»

Von dieser Adressierungs-Art wird abgeraten – sie sollte nur verwendet werden, wenn der OPC UA Server nur Namen in einer Sprache unterstützt und der Browse-Name nicht ausreichend aussagekräftig ist.

Mögliche Datentypen:

- BOOL (Boolean)
- BYTE (Byte)
- SINT (SByte)
- WORD, UINT (UInt16)
- DWORD, UDINT (UInt32)
- INT (Int16)
- DINT (Int32)
- LINT (Int64)
- ULINT (UInt64)
- REAL (Float)
- LREAL (Double)
- STRING (String)
- DATETIME
- Arrays
- History-Listen für Zeitdiagramme

Beispiel-Adressen im Unified-E App Designer:



Bit-Adressierung bei numerischen Variablen:

Beispiel: Demo/Static/Byte.0 adressiert das erste Bit.