



Mit Sicherheit – **OPC Unified Architecture**

Sichere Kommunikation mit der IEC 62541

OPC Unified Architecture



ÜBERSICHT OPC UA

→ OPC Unified Architecture (OPC UA) ist die neue Technologiegeneration der OPC Foundation für einen sicheren, zuverlässigen und herstellereu-

tralen Transport von Rohdaten und vorverarbeiteten Informationen von der Fertigungsebene bis in das Produktionsplanungs- oder ERP-System. Auf einheitliche, sichere und zuverlässige Weise steht mit OPC UA jeder berechtigten Anwendung und jeder autorisierten Person jede gewünschte Information zu jeder Zeit und an jedem Ort zur Verfügung. Diese Funktion ist unabhängig davon, von welchem Hersteller die Anwendungen stammen, in welcher Programmiersprache sie entwickelt wurden oder auf welchem Betriebssystem sie eingesetzt werden. Auf der Basis einer Service-orientierten Architektur (SOA) bildet OPC UA die Brücke zwischen der Unternehmensleitenebene und eingebetteten Automatisierungskomponenten. ■

Sicherheitskonzepte

Sicherheit war eine zentrale Anforderung bei der Entwicklung von OPC UA. Sie wird in verschiedenen Bereichen adressiert:

AUTHENTIFIZIERUNG UND AUTORISIERUNG VON BENUTZERN

→ Beim Verbindungsaufbau identifiziert sich der Benutzer über

- X.509 Zertifikate
- Benutzer / Password
- oder Kerberos

Damit werden alle gängigen Benutzerverwaltungssysteme wie Microsoft Active Directory unterstützt. Des Weiteren können die Zugriffsrechte (zum Beispiel

lesen und schreiben von Werten) feingranular pro Benutzer angegeben werden.

INTEGRITÄT

→ Das Signieren der Nachrichten verhindert das Ändern des Inhalts einer Nachricht durch einen Dritten. So wird verhindert, daß beispielsweise eine Schreib-anweisung zum Öffnen eines Schalters durch einen Dritten verfälscht wird und der Schalter statt dessen geschlossen wird.

Open

- > 450 Mitglieder
- Plattformneutral
- Alle Anwendungsbereiche
- Alle Verbindungen

Productivity

- Industriestandard
- Herstellerübergreifend
- Interoperabilität
- Zuverlässigkeit

Collaboration

- Device Integration
- IEC 61131-3 / PLCopen
- Analyzer Device Integration
- ISA-95, ISA-88
- MTConnect
- Smart Grid
- Field Device Integration
- EDDL und FDT

ANSCHRIFT:

OPC Foundation
16101 N. 82nd Street
Suite 3B
Scottsdale, AZ 85260-1868
USA

KONTAKT:

Phone: (1) 480 483-6644
Fax: (1) 480 483-7202
office@opcfoundation.org

INFORMATIONEN:

www.opcfoundation.org

KOOPERATION:

- PLCopen
- ISA
- MTConnect
- FDT
- PNO
- HART
- FF



Sicherheitskonzepte

Sicherheit war eine zentrale Anforderung bei der Entwicklung von OPC UA. Sie wird in verschiedenen Bereichen adressiert:

VERTRAULICHKEIT

→ Die Vertraulichkeit der ausgetauschten Information wird durch die Verschlüsselung der ausgetauschten Nachrichten sichergestellt. Dabei werden moderne Kryptographie-Algorithmen verwendet. Um auch den zukünftigen Sicherheitsanforderungen gewachsen zu sein können im nachhinein noch stärkere und modernere Algorithmen einer Anwendungen hinzugefügt werden, ohne das Protokoll zu verändern.

Entsprechend der Anforderungen der jeweiligen Anwendung können verschiedene Sicherheitsstufen gewählt werden. In einigen Bereichen ist es ausreichend die Nachrichten zu signieren um Änderungen durch Dritte auszuschließen, in anderen Fällen dürfen Daten auch nicht von Dritten gelesen werden und ein zusätzliches Verschlüsseln der Nachrichten ist erforderlich.

AUTHENTIFIZIERUNG UND AUTORISIERUNG VON ANWENDUNGEN

→ OPC UA Anwendungen identifizieren sich (ähnlich wie bei einem Benutzer) über so genannte Software- und Applikationsinstanz-Zertifikate.

Mit Hilfe von Software-Zertifikaten ist es möglich bestimmten Client Anwendungen einen erweiterten Zugriff auf Informationen eines OPC UA Servers zu geben, beispielsweise für das Engineering eines OPC UA Servers.

Durch Applikationsinstanz-Zertifikate kann sichergestellt werden, daß ein OPC UA Server nur mit vorkonfigurierten Clients kommuniziert. Ein Client kann durch das Applikationsinstanz-Zertifikat des Servers sicherstellen, daß er mit dem richtigen Server spricht (ähnlich der Zertifikate eines Web-Browsers).

Die Berücksichtigung dieser Zertifikate ist optional, d.h. ein OPC UA Server kann auch jedem Client den gleichen Zugriff abhängig der Benutzerrechte geben. ■

MEHR INFORMATION UNTER

www.opcfoundation.org

