V1.1 GB

OPC FOUNDATION – **WWW.OPCFOUNDATION.ORG**

OPC Unified Architecture

Secure communication with IEC 62541 OPC UA

OVERVIEW OF OPC UA

→ OPC Unified Architecture (OPC UA) is the new technology generation of the OPC Foundation for the secure, reliable and manufacturer-neutral transport of raw data and pre-processed information from the manufacturing level into the production planning or ERP system.

With OPC UA, all desired information is available to every authorised application and every authorised person at any time and in any place. This function is independent of the manufacturer from which the applications originate, the programming language in which they were developed or the operating system on which they are used. On the basis of a service-orientated architecture (SOA), OPC UA forms the bridge between the company management level and embedded automation components. ■

Secure concepts

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

AUTHENTICATION AND AUTHORISATION OF USERS

→ On establishing a connection, the user identifies himself via

- X.509 certificates
- User name / password
- or Kerberos

Thus all common user administration systems such as Microsoft Active Directory are supported.

Furthermore, the access rights (for example for the reading and writing of values) can be specified in a fine-grained manner per user.

INTEGRITY

→ The signing of messages prevents a third party from changing the contents of a message.

This prevents, for example, a write statement to open a switch being falsified by a third party and the switch being closed instead.

Open

- > 450 members
- Platform-neutral
- All areas of application
- All connections

Productivity

- Industry standard
- Manufacturer-independent
- Interoperability
- Reliability

Collaboration

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

ADDRESS:

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

CONTACT:

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

INFORMATION:

www.opcfoundation.org

COOPERATION:

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

Security concepts

Security was a central requirement in the development of OPC UA. It is addressed in various areas:

CONFIDENTIALITY

→ The confidentiality of the exchanged information is secured by the encryption of the exchanged messages. Modern cryptographic algorithms are used for this. In order to be able to cope with future security requirements as well, even stronger and more modern algorithms can subsequently be added to an application without changing the protocol.
Different security levels can be selected according to the requirements of the respective application. In some areas it is sufficient to sign the messages in order to prevent changes being made by third parties, while additional coding of the messages is necessary in other cases where the data must also not be read by third parties.

AUTHENTICATION AND AUTHORISATION OF APPLICATIONS

→ OPC UA applications identify themselves (in a similar way to a user) via so-called software and application instance certificates.
With the aid of software certificates it is possible to grant certain client applications extended access to the information on an OPC UA server, for example for the engineering of an OPC UA server.
Application instance certificates can be used to ensure that an OPC UA server communicates only with preconfigured clients. A client can ensure by means of the server's application instance certificate that it is speaking to the correct server (similar to the certificates of a Web browser).
The taking into account of these certificates is optional, i.e. an OPC UA server can also grant the same access to each client, depending on the user rights. ■

MORE INFORMATION

www.opcfoundation.org