



V1.1 F

OPC FOUNDATION – WWW.OPCFFOUNDATION.ORG

OPC Unified Architecture – Communication sécurisée selon IEC 62541 OPC UA



APERCU D'OPC UA

→ OPC Unified Architecture est la nouvelle génération technologique de la Fondation OPC . Il permet le transport de données brutes ou prétraitées du niveau production au niveau planification ou système ERP, de manière sûre, fiable et indépendante du fabricant.

Avec OPC UA, toutes les informations sont disponibles pour chaque application et personne autorisée, à tout moment et en tout lieu. Cette fonction est indépendante des fabricants de composants, du langage de programmation ou du système d'exploitation utilisé. Basé sur une architecture orientée objet, OPC UA fait le lien entre le niveau entreprise et les composants d'automatisation embarqués. ■

Concepts de sécurité

La sécurité était une exigence principale dans le développement d' OPC UA. Elle est nécessaire pour différents domaines :

AUTHENTIFICATION ET AUTORISATION DES UTILISATEURS

→ Pour établir une connexion, l'utilisateur s'identifie par

- Certificats X.509
- Nom d'utilisateur / mot de passe
- Kerberos

Ainsi, tous les systèmes d'administration d'utilisateurs comme Microsoft Active Directory sont supportés. De plus, les droits d'accès (par exemple l'accès aux données en lecture et en écriture) peuvent être spécifiés pour chaque utilisateur.

INTEGRITE

→ La signature de messages empêche un tiers d'en modifier le contenu. Cela évite, par exemple, à une instruction d'ouverture d'un contacteur d'être falsifiée et d'actionner sa fermeture à la place. ■

Ouvert

- > 450 membres
- Indépendant de la plateforme
- Pour toutes les applications
- Pour toutes les connexions

Productivité

- Standard industriel
- Indépendant du fabricant
- Interopérable
- Fiable

Collaboration

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

ADRESSE :

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

CONTACT :

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

INFOMATION :

www.opcfoundation.org

COOPÉRATION :

- PLCopen
- ISA
- MTCconnect
- FDT
- PNO
- HART
- FF



Concept de sécurité

**La sécurité était une exigence principale dans le développement d' OPC UA.
Elle est nécessaire pour différents domaines :**

CONFIDENTIALITE

→ La confidentialité des informations échangées est assurée par le cryptage des messages. On utilise pour cela des algorithmes modernes. Afin d'être en mesure de faire face aux exigences de sécurité futures, plus forte et plus moderne, d'autres algorithmes peuvent ensuite être ajoutés sans modifier le protocole. Différents niveaux de sécurité peuvent être sélectionnés selon les exigences de l'application concernée. Pour certaines, il suffit de signer les messages afin de prévenir les changements apportés par des tiers, tandis que le codage des messages est nécessaire dans d'autres cas pour ne pas autoriser la lecture ou la modification de l'application.

AUTHENTIFICATION ET AUTHORISATION DES APPLICATIONS

→ Les applications OPC UA d'identifient elles-mêmes (d'une manière similaire à un utilisateur) via ce que l'on appelle des « software and Application instance certificats ».

Avec l'aide de ces certificats logiciels, il est possible d'accorder, à certaines applications client, un accès étendu à l'information sur un serveur OPC UA, par exemple pour l'ingénierie d'un serveur OPC UA.

Ces certificats peuvent être utilisés pour s'assurer qu'un serveur OPC UA communique uniquement avec les clients préconfigurés. Un client peut s'assurer, au moyen du certificat du serveur d'application qu'il communique avec le bon serveur (similaire aux certificats d'un navigateur Web).

La prise en compte de ces certificats est en option, à savoir qu'un serveur OPC UA peut également accorder le même droit accès à chaque client, en fonction des droits de l'utilisateur. ■

PLUS INFORMATION :

www.opcfoundation.org

