V1.1 SP

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

OPC Unified Architecture:

Comunicaciones seguras con IEC 62541 OPC UA

RESUMEN DE OPC UA

→ OPC Unified Architecture es la nueva generación tecnológica propuesta por OPC Foundation para la transmisión segura, fiable – y neutra con respecto al fabricante – de datos en bruto y/o información pre procesada entre los niveles de producción y los sistemas de planificación de producción (MES) y de empresa (ERP).

Con OPC UA, toda la información deseada estará disponible para cualquier aplicación y usuario autorizados, en cualquier instante y en cualquier lugar. Esta funcionalidad será independiente del fabricante que haya desarrollado la aplicación, el lenguaje de programación seleccionado y el sistema operativo utilizado.

Sobre la base de una arquitectura orientada a servicios (SOA), OPC UA constituye el nexo de unión entre los niveles de gestión de la empresa y los sistemas de automatización embebidos. ■

Conceptos de seguridad

La seguridad ha sido un requisito esencial en el desarrollo de OPC UA. Se ha abordado en varias áreas:

AUTENTIFICACIÓN Y AUTORIZACIÓN DE USUARIOS

→ Cuando se establece una conexión, el usuario se identifica a sí mismo mediante

- Certificados X.509
- Usuario / contraseña
- o Kerberos

Así, todos los sistemas de administración centralizada de usuarios –como Microsoft Active Directory– son compatibles. Por otra parte, los derechos de acceso (por ejemplo, lectura o escritura de variables) pueden especificarse, de forma individual, para cada usuario.

INTEGRIDAD

→ La firma de los mensajes impide que un tercero pueda modificar su contenido. Esto impide, por ejemplo, que un tercero pueda falsificar un comando de apertura de un dispositivo para enviar una orden de cierre.

Open

- > 450 miembros
- Independiente de la plataforma
- Todas las áreas de aplicación
- Todas las conexiones

Productivity

- Estándar de la industria
- Independiente del fabricante
- Interoperable
- Fiable

Collaboration

- Integración en dispositivos
- IEC 61131-3 / PLCopen
- Integración con dispositivos analizadores
- ISA-95, ISA-88
- MTConnect
- Smart Grid (Redes Inteligentes)
- Integración con dispositivos de campo
- EDDL y FDT

DIRECCIÓN:

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

DATOS DE CONTACTO:

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

INFORMACIÓN:

www.opcfoundation.org

COOPERACIÓN:

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

Conceptos de seguridad

La seguridad ha sido un requisito esencial en el desarrollo de OPC UA. Se ha abordado en varias áreas:

CONFIDENCIALIDAD

→ La confidencialidad de la información intercambiada se garantiza mediante el cifrado de los mensajes que se envían. Para ello se utilizan las más modernas técnicas criptográficas. Con el fin de poder hacer frente -en el futuro- a requisitos de seguridad más exigentes, es posible implementar en la aplicación algoritmos de cifrado más modernos –y seguros- sin tener que cambiar el protocolo.
Pueden seleccionarse diferentes niveles de seguridad de acuerdo con los requisitos de cada aplicación. En algunas zonas será suficiente firmar los mensajes para evitar cambios realizados por terceros, mientras que en otras será necesaria una codificación adicional con objeto de evitar que éstos puedan ser descifrados.

AUTENTIFICACIÓN Y AUTORIZACIÓN DE APLICACIONES

→ Las aplicaciones OPC UA se identifican a sí mismas (de forma similar a como lo hacen los usuarios) mediante los, así llamados, certificados de instancias de software y aplicaciones.
Con la ayuda de los certificados de software es posible permitir a ciertas aplicaciones cliente acceso extendido a la información disponible en el servidor OPC UA para, por ejemplo, realizar labores de ingeniería en dicho servidor OPC UA.
Los certificados de instancias de aplicación pueden utilizarse para asegurar, por ejemplo, que un servidor OPC UA sólo se comunique con un conjunto de clientes preconfigurado. O un cliente asegurarse, por medio del certificado de instancia de aplicación del servidor, que está intercambiando información con el servidor adecuado (similar al uso de certificados en un navegador web).
La toma en consideración de estos certificados es opcional, es decir, un servidor OPC UA también puede conceder derechos de acceso a la aplicación cliente en función de los derechos que tiene su usuario. ■

MÁS INFORMACIÓN

www.opcfoundation.org