VI JORNADAS sobre Tecnologías y Soluciones para la Automatización Industrial
Vigo, 3 al 7 de noviembre de 2014
Universidade de Vigo | Escola de Enxeñaría Industrial

5ª SESIÓN

LOGITEK

MIÉRCOLES 5, 18:50-20:00

Comunicaciones industriales seguras con OPC UA

Ponente:

- **D. Héctor García**
  (Industrial Communications Manager, LOGITEK)

Industrial Communications by LOGITEK

1. Acerca de Logitek y Kepware
2. Túneles OPC-UA
3. Seguridad en OPC-UA
4. Túnel seguro con Kepware
5. Conclusiones

Acerca de Logitek

Industrial Communications
by LOGITEK

- Referencia en el mercado español desde 1979 ayudando a nuestros clientes a alcanzar la excelencia operativa y la reducción de costes
- Especialistas en sistemas de control, comunicaciones, gestión a tiempo real y ciberseguridad en entornos industriales e infraestructuras
- Especialistas en capturar, analizar, discriminar y mostrar la información más relevante para una toma de decisiones inmediata y libre de incertidumbres

Acerca de Logitek

Industrial Communications by LOGITEK

Competence Center

Consultoría-Formación-Soporte

Control | Telecontrol | Movilidad | OPC | M2M / IoT | Redes Industriales | Alta Disponibilidad | Scada/MES | Reporting | Cloud Computing

Ciberseguridad | Gestión Tiempo Real | Comunicaciones | Instalaciones

Logitek

Industrial Communications
by LOGITEK

División dentro de Logitek dedicada a la comunicación entre dispositivos, procesos y sistemas

Entre dispositivos y sistemas

OPC®

Entre dispositivos

PROFIBUS®

PROFINET®

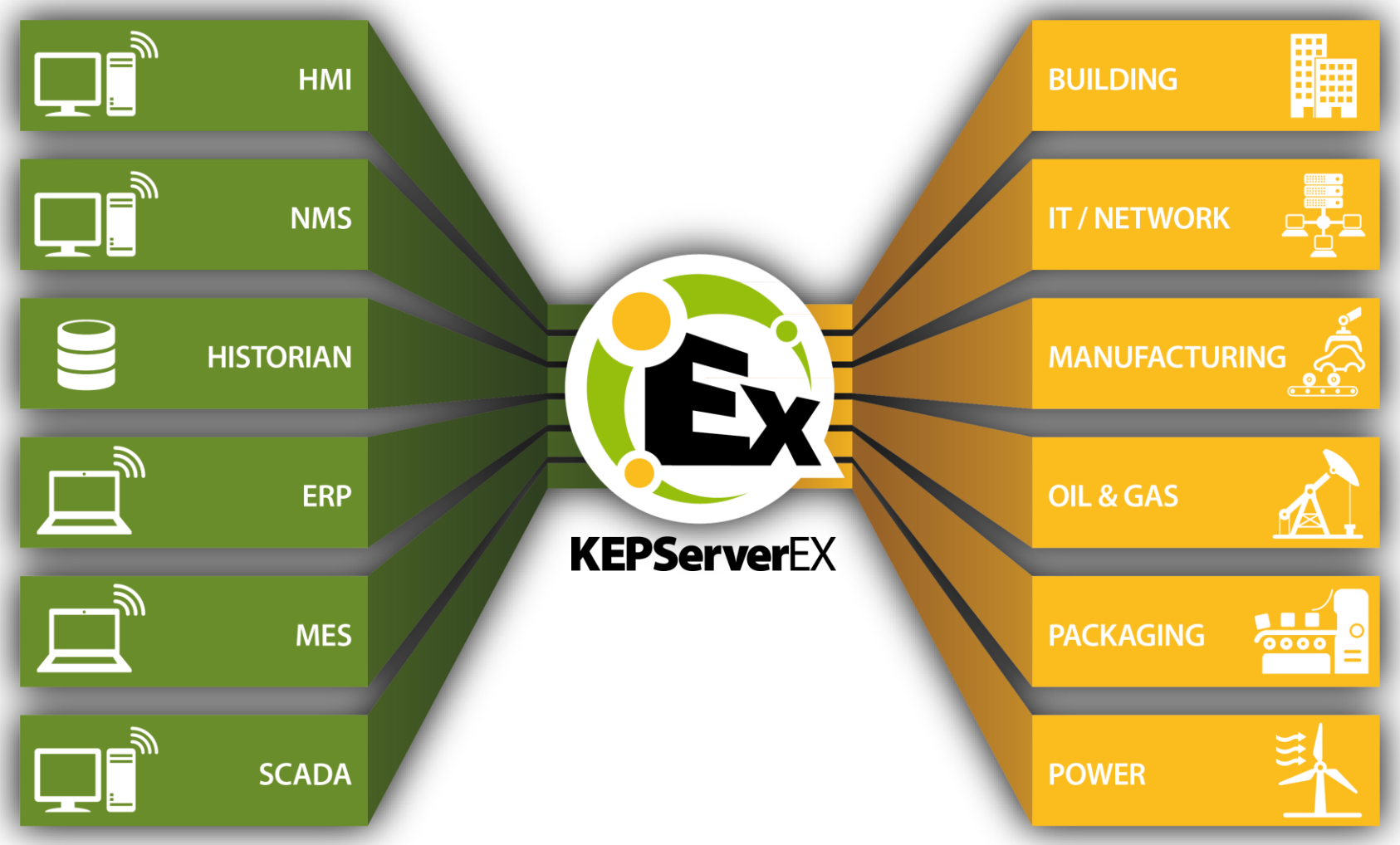
Kepware Technologies

Industrial Communications by LOGITEK

- Proveedor de un software para comunicación industrial utilizado en entornos discretos, procesos y lotes
- Su punto fuerte es el intercambio de información entre aplicaciones y/o dispositivos

Kepware Technologies

Industrial Communications by LOGITEK



Industrial Communications by LOGITEK

1. Acerca de Logitek y Kepware
2. **Túneles OPC-UA**
3. Seguridad en OPC-UA
4. Túnel seguro con Kepware
5. Conclusiones

Antes de OPC

Industrial Communications by LOGITEK

- Cada aplicación su propio driver
- Poca Integración
- Soluciones propietarias

¿Dónde están los datos?

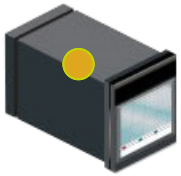
¿Adaptación a cambios?

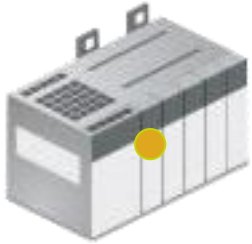
La solución OPC

Industrial Communications by LOGITEK

ERP

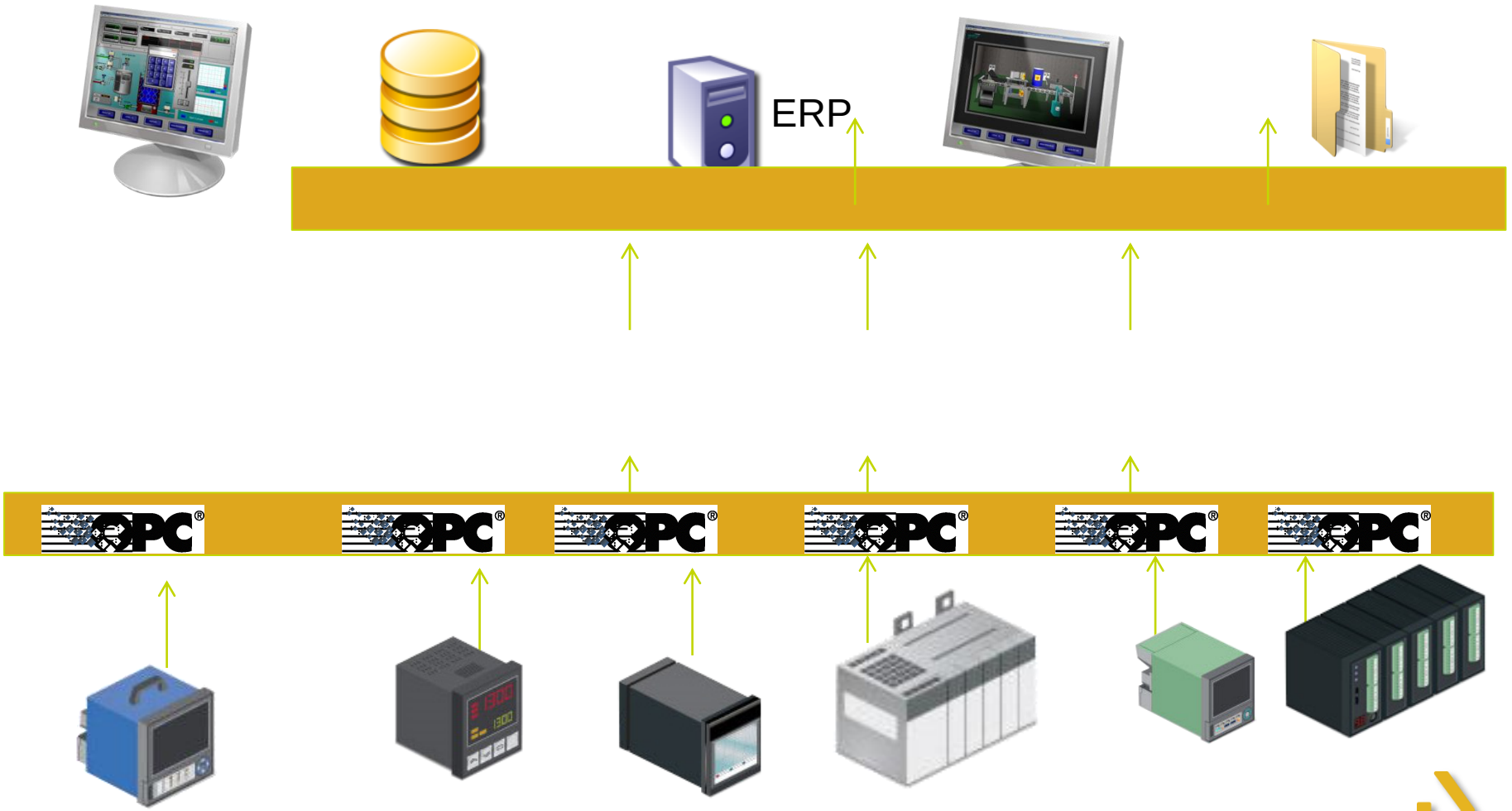
Informes





La solución OPC

Industrial Communications
by LOGITEK



Características OPC

Industrial Communications by LOGITEK

- Especificación pública, no propietaria
- Arquitectura Cliente/Servidor
- Envío de datos como texto plano
- Basado en Microsoft ActiveX y COM/DCOM

¿Protocolo Seguro?

Industrial Communications by LOGITEK

- Modbus TCP, el protocolo industrial más utilizado
  - Mucha documentación del protocolo
  - Puerto 502
  - Direcciones de memoria fijas
  - Mensajes sin codificar

¿Por qué no es seguro?

Industrial Communications by LOGITEK

- Cualquiera podría leer los datos y entenderlos
- Cualquiera podría hacerse pasar por el maestro o por el esclavo
- Cualquiera podría modificar los mensajes

¿Qué es un túnel?

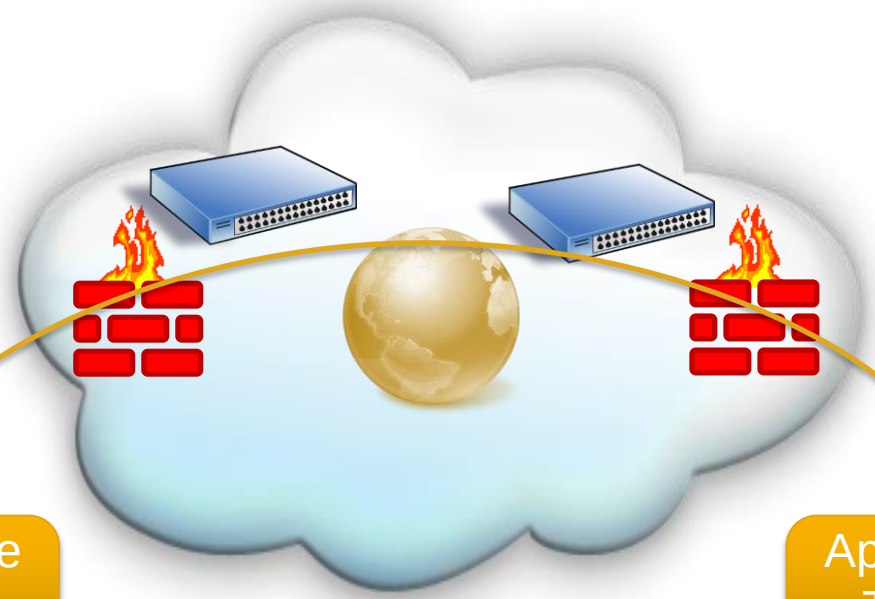
Industrial Communications by LOGITEK

¿Qué significa “tunneling” en este contexto?

Crear un canal de comunicación entre dos puntos a través de barreras

¿Cómo es un túnel?

Industrial Communications by LOGITEK



Aplicación de Tunneling Cliente

Aplicación de Tunneling Servidor

Protocolo cliente

Protocolos dispositivos

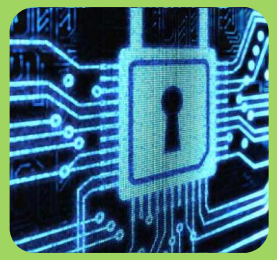
¿Por qué crear un túnel?

Industrial Communications by LOGITEK

Habilitar comunicaciones entre redes, routers o Firewalls (por ejemplo Internet)

Quizás para:

- Permitir a un cliente OPC-DA en un red comunicar con un dispositivo o un servidor OPC-DA en otra red
- Permitir a un cliente No-OPC comunicar con un dispositivo o un servidor OPC en otra red
- Permitir a un dispositivo en una red comunicar con otro dispositivo en otra red



Añadir seguridad a las comunicaciones

- Algunos protocolos son abiertos y comprensibles por cualquiera con una guía (por ejemplo, Modbus)

Un buen protocolo para tunneling

Industrial Communications by LOGITEK

Fácil configuración	Debe ser más sencillo de configurar que DCOM
Firewall-Friendly	Los puertos deberían ser configurables
Seguro	Debería autentificar la conexión y encriptar la información
Comandos flexibles	Debe soportar recoger cambios de valores en bloque y lecturas bajo demanda
Mensajes asíncronos	Debe procesar los comandos de manera eficiente y no retardar a otros clientes o al servidor
Fácil diagnóstico	Debe seguir los estándares y tener la capacidad de ser analizado por herramientas de red

OPC-UA

- Nueva especificación de OPC Foundation que mejora OPC clásico (IEC-62541)
  - Integra las especificaciones clásicas (DA, HDA, etc.)
  - Independiente de la plataforma (S.O)
  - Permite el uso de estructuras
  - Seguridad nativa

Necesidad de Seguridad

Industrial Communications by LOGITEK

- Para tomar las mejores decisiones, la información debe estar disponible a cualquiera, en cualquier lugar y en cualquier momento
- La información crítica viaja por dominios públicos
- Debemos asegurar que solo las aplicaciones, dispositivos y usuarios autorizados acceden a la información

Objetivos de la Seguridad

Industrial Communications by LOGITEK

- *Auditabilidad – Permite trazar todas las acciones realizadas, por quién y cuándo*
- *Autenticación – Permite a las partes probar su identidad como parte de una relación de confianza*
- *Autorización – Marca las restricciones de acceso adecuadas a las partes autenticadas*

Objetivos de la Seguridad

- *Disponibilidad – Limita los factores que pueden afectar el tiempo de ejecución*
- *Confidencialidad – Asegura que la información intercambiada está oculta para las partes no autorizadas*
- *Integridad – Asegura que la información intercambiada no sufre alteraciones*

Anemazas

- *Credenciales Comprometidas – Permite a un atacante asumir una identidad válida*
- *Eavesdropping – Permite la interceptación de información confidencial*
- *Malformación de Mensajes – Puede causar que el recepetor del mensaje realice tareas inadecuadas o Denegación de Servicio* (DoS)

Amenazas

Industrial Communications by LOGITEK

- *Alteración de Mensajes/Spoofing* – Permite la falsificación de mensajes basándose en la documentación del protocolo
- *Message Flooding* - Envío masivo de mensajes a un objetivo para afectar su disponibilidad (DoS)
- *Repetición de Mensajes – Reenviar mensajes en el futuro para realizar tareas válidas, pero en momento inadecuado*

Amenazas

Industrial Communications by LOGITEK

- *Profiling* - Un atacante puede utilizar ciertas vulnerabilidades conocidas y publicadas
- *Secuestro de Sesión – Permite a un atacante ponerse en medio de dos partes ya identificadas para coger el control*

Seguridad en Planta

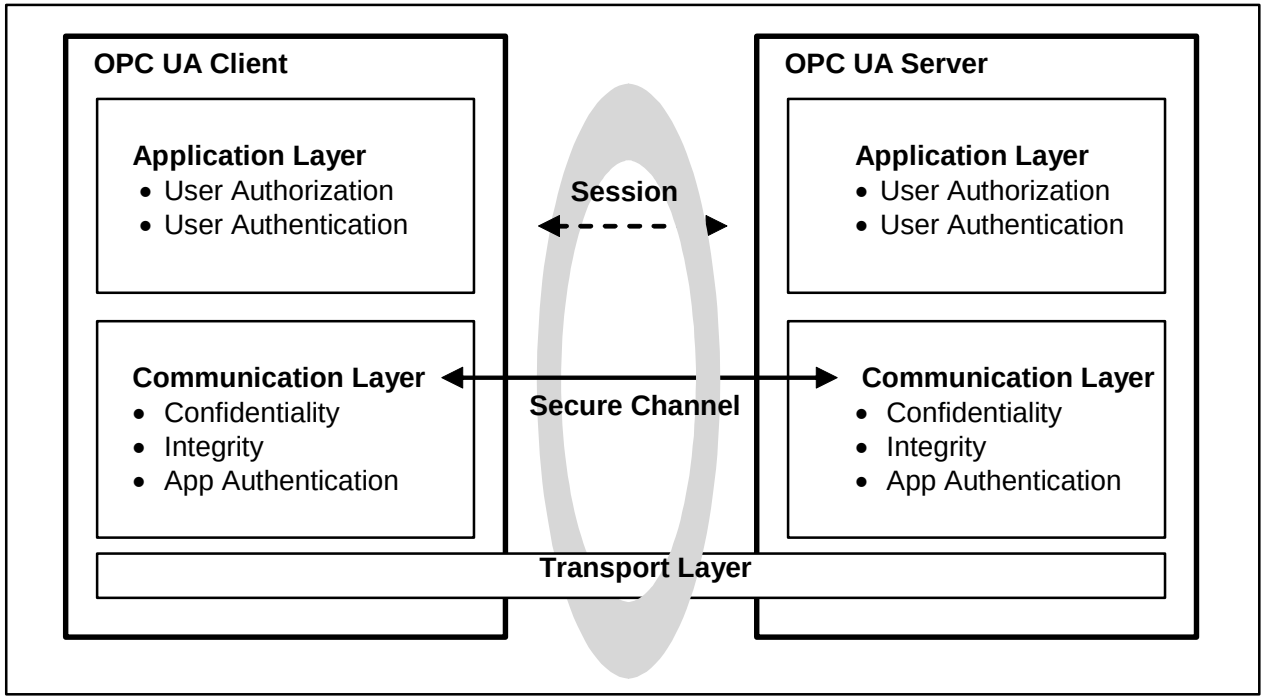
Industrial Communications by LOGITEK

- *Cyber Security Management System (CSMS)*
  - Políticas de seguridad en las fronteras
  - Requerimientos de auditabilidad
  - Procedimientos preventivos y correctivos

Seguridad en Planta

- *Defensa en profundidad*
  - Múltiples capas de protección, asumiendo que no existe una solución única
  - Puede incluir reglas generales IT, firewalls, Sistemas de Prevención/Detección de Intrusos (IDS/IPS), Parches , Sistemas de gestión, …

- *OPC-UA - Diseño multi capa:* Aplicación, Comunicación y Transporte



- *Capa de aplicación*
  - Maneja la mayoría de la funcionalidad OPC (lecturas, escrituras, …)
  - Gestión para la autenticación y autorización de usuarios a través del concepto de sesión entre aplicación cliente y servidor

Arquitectura de Seguridad

Industrial Communications by LOGITEK

- *Capa de Comunicación*
  - Canal seguro entre cliente y servidor para autenticación de aplicaciones, confidencialidad e integridad
  - Intercambio de certificados digitales para la autenticación de aplicaciones
  - Encriptación para la confidencialidad
  - Firma de mensajes para la integridad

- *Capa de Transporte*
  - Maneja el envío y recepción de los mensajes entre aplicaciones
  - Puede implementar canales seguros gestionados por la capa de Comunicación

OPC UA: Cómo funciona

Industrial Communications by LOGITEK

- *Certificado de Instancia de la Aplicación*
  - Certificado digital único X.509 asignado durante la instalación
  - Puede ser regenerado
  - Compuesto por una pareja de claves Pública y Privada
  - Las claves varían en longitud (cuanto más larga la clave, mayor es la seguridad)

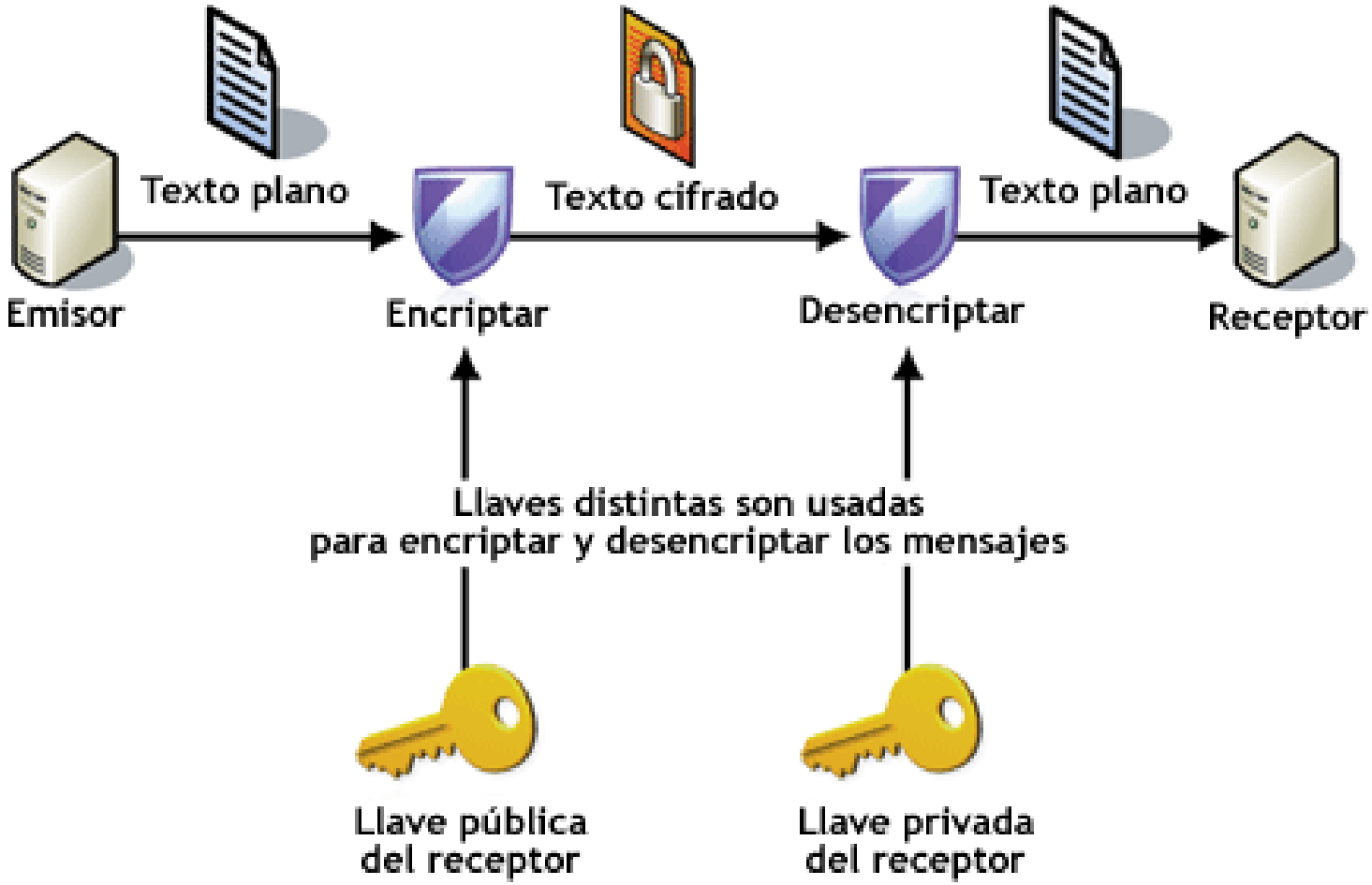
OPC UA: Cómo funciona

Industrial Communications by LOGITEK

- *Canal Seguro*
  - Un cliente se conecta a un servidor en inmediatamente genera un canal seguro
  - Requiere que el cliente y servidor intercambien información segura para la posterior comunicación
  - Se debe configurar para que cliente y servidor confíen en el certificado del otro
  - Este procedimiento permite la autenticación de la aplicación

OPC UA: Cómo funciona

Industrial Communications by LOGITEK



OPC UA: Cómo funciona

Industrial Communications by LOGITEK

- *Sesión*
  - Un cliente crea una sesión que gestiona el canal seguro previamente creado
  - Requiere que la identidad del usuario de la aplicación sea conocido por ambas partes
  - Provee al usuario de la autorización (qué puede hacer y qué no)

Reducir amenazas

- *Canal seguro / Sesión*
  - Protege contra eavesdropping
  - Protege contra alteración de mensajes/spoofing
  - Protege contra la detección de credenciales de usuario
  - Todo mediante el uso de claves Públicas/Privadas, firma digital y encriptación

Reducir amenazas

- *Especificación diseñada para la seguridad*
  - Los clientes están limitados en qué acciones pueden realizar antes de ser autenticados
  - Acceso a información de seguridad y conexión, la cual es estática y requiere poco procesamiento
  - Comportamiento predefinido del servidor ante intentos erróneos y repetidos de creación de canales seguros
  - Protege contra message flooding

Reducir amenazas

- *Detalles en los mensajes*
  - Cada mensaje contiene un ID de sesión, ID de canal seguro, ID de transacción, Fecha y hora y número de secuencia, que no son modificables
  - Los clientes y servidores deben validar cada mensaje
  - Protege contra la repetición de mensajes
  - Protege contra malformación de mensajes

Industrial Communications by LOGITEK

1. Acerca de Logitek y Kepware
2. Túneles OPC-UA
3. Seguridad en OPC-UA
4. **Túnel seguro con Kepware**
5. Conclusiones

Tunel con KepServerEx

Industrial Communications by LOGITEK

PC: ClienteUA
S.O: Win XP

PC: Server1
S.O: Windows 2003

1. Instalar KepServerEx en Server1 con el driver del PLC
2. Instalar KepServerEx en ClienteUA con el driver OPC-UA Client
3. Configurar un Endpoint en Server1
4. Configurar OPC-UA Client driver en la máquina cliente
5. Importar en el cliente los tags del servidor

Vídeo

Industrial Communications by LOGITEK

1. Acerca de Logitek y Kepware
2. Túneles OPC-UA
3. Seguridad en OPC-UA
4. Túnel seguro con Kepware
5. **Conclusiones**

Conclusiones

Industrial Communications by LOGITEK

- OPC-UA permite la interoperabilidad entre software y hardware de diferentes fabricantes
- La interoperabilidad permite el intercambio de información crítica de cualquier sistema de control industrial
- Para poder tomar la decisiones adecuadas, se necesita la información inmediata y en cualquier lugar

Conclusiones

Industrial Communications by LOGITEK

- El envío de datos por dominios públicos debe hacerse de forma segura para proteger la auntenticidad, integridad y confidencialidad de la información
- OPC-UA “toma prestados” principios y técnicas habituales en el mundo IT, los cuales posibilitan el intercambio seguro de información

Industrial Communications
by LOGITEK

GRACIAS

Ponente:

- **D. Héctor García**
  (Industrial Communications Manager, LOGITEK)
  hector.garcia@logitek.es

Universidade de Vigo - E.E.I. Escola de Enxeñaría Industrial - JAI 2014