Revista Conectividad
Julio-diciembre 2022 *ISSN:2806-5875*
pp. 56-74 *Correo: revista@ister.edu.ec*
Volumen 3, Número 2

Variantes de la Tecnología OPC-UA y su utilización en la interconexión de Controladores Industriales con diferentes protocolos de comunicación

Variants of OPC-UA Technology and its use in the interconnection of Industrial Controllers with different communication protocols.

Fernando Jácome[1], Luis Daniel Andagoya-Alba[2], Rommel Valencia[3], Henry Osorio[4], Edison Paredes[5]

[1] Next Generation Plant Services, fjacome@nps-tech.com
[2] Instituto Tecnológico Universitario Rumiñahui, luis.andagoya@ister.edu.ec
[3] Rhelec Ingeniería CIA LTDA, rommel.valencia@rhelec.ec
[4] DTV TELECOM CIA. LTDA, hosorio@dtv.ec
[5] Instituto Tecnológico Universitario Rumiñahui, edison.paredes@ister.edu.ec

Autor para correspondencia: fernandojacomes@hotmail.com

Fecha de recepción: febrero 2022 ***Fecha de aceptación:*** mayo 2022

RESUMEN

En el área industrial existe una variabilidad de tecnologías controladores con diversas características, dificultando de esta forma su intercomunicación e interoperabilidad, debido a esto se ha propuesto la tecnología OPC-UA como una alternativa que permite la intercomunicación entre controladores de diferentes fabricantes. El presente trabajo tuvo como objetivo el análisis del uso de esta tecnología para la intercomunicación de controladores industriales con diferentes protocolos de comunicación, el método utilizado fue a través del análisis de casos de estudios con diferentes características referentes a seguridades, cifrado y firma digital. Los resultados mostraron que el uso del sistema de comunicación OPC-UA redujo las complejidades de configuración ya que soporta sistemas abiertos, toleró cortafuegos y la configuración. Permitiendo la validación inmediata de variables desde el sistema SCADA hasta los controladores industriales sin previa configuración. Con esto se concluyó que la comunicación OPC-UA puede reemplazar eficazmente al sistema tradicional OPC.

Palabras clave: Tecnología OPC-UA, intercomunicación, protocolo de comunicación, controlador industrial.

ABSTRACT

In the industrial area there is a choice of controller technologies with different characteristics, which makes this form of intercommunication and interoperability difficult, due to this OPC-UA technology has been proposed as an alternative that allows intercommunication between controllers from different manufacturers. The objective of this work is to analyze the use of this technology for the intercommunication of industrial controllers with different communication protocols through the analysis of case studies with different characteristics regarding security, encryption and digital signature. The results showed that the use of the OPC-UA communication system reduced the configuration complexities as it supported open systems, tolerated firewalls and configuration. Allowing the immediate validation of variables from the SCADA system to the industrial controllers without prior configuration. With this it can be concluded that the OPC-UA communication can successfully replace the traditional OPC system.

Key words: OPC-UA technology, intercommunication, communication protocol, industrial controller.

INTRODUCCIÓN

Dentro del área industrial existe una gran cantidad de mecanismos de comunicación entre controladores y sistemas SCADA, dependiendo de las aplicaciones y de los procesos a controlar se pueden tener controladores de diferente fabricante provocando que en una misma industria se tenga diferentes protocolos de comunicación, dificultando de esta forma su intercomunicación e interoperabilidad. Adicionalmente se debe tener en cuenta la seguridad que estos procesos de intercomunicación deben tener para evitar posibles ataques que pueden dañar los procesos afectando a las maquinas que forman parte de los mismos. Por lo cual es necesario validar la tecnología óptima para su procesamiento. (Eckhardt et al., 2018; Yuan et al., 2021). Para solucionar este inconveniente se ha propuesto la tecnología OPC-UA como una alternativa que permite la intercomunicación entre controladores de diferentes fabricantes de forma segura, eficiente y confiable. Estas características han posicionado a esta tecnología como una posible solución al inconveniente de la intercomunicación entre distintos controladores con distintos protocolos de comunicación (Germany, s. f.; *OPC UA_test*, s. f.; Schwarz & Börcsök, 2013).

La tecnología OPC-UA se basa principalmente en una arquitectura cliente-servidor, la cual puede tener diferentes aplicaciones que van desde procesos de intercomunicación entre controladores industriales hasta el manejo de negocios. Una aplicación que está tomando mucha relevancia es su aplicabilidad en sistemas de Smart Grid debido a su uso en el modelado de la información y sus procesos de comunicación (Eymüller et al., 2020; Lai et al., 2020; Okuda et al., 2017).

La tecnología OPC-UA permite una estandarización de intercambio de datos de forma determinística, rápida y segura con una aceptación universal debido a que puede ser implementado en diferentes tipos de hardware como ordenadores industriales, controladores lógicos programables, microcontroladores y servidores en la nube, de igual forma en diferentes sistemas operativos como Microsoft Windows, Android, Linux y Apple OSX. Utiliza varios protocolos, cifrados y monitoreo de tiempos de espera. Todo esto permite la intercomunicación entre productos de distintos fabricantes (Drahoš et al., 2018; Marksteiner, 2018; Muennoi & Hormdee, 2016).

Para el desarrollo de la estandarización propuesta por esta tecnología se requiere de un análisis que permita determinar las características de funcionamiento de los diversos servicios y conceptos desarrollados por los grupos de trabajo de la tecnología OPC-UA en comparación con las tecnologías aplicadas actualmente. Es necesario determinar si esta tecnología propuesta puede ser una alternativa que perdure en el tiempo y contemple la apertura a las futuras tecnologías, esto debido a que los desarrollos futuros pueden dar de baja a los sistemas actuales no solo en los elementos a intercomunicar sino también en la propia tecnología OPC-UA debido a las posibles actualizaciones que podrían irse desarrollando. Así mismo es importante analizar la infraestructura de comunicaciones que le permitiría a esta tecnología la integración de los controles de los procesos en la industria de forma eficiente, segura y con un costo mínimo de implementación y de migración desde los procesos actuales (Almeida, s. f.; Han et al., 2022; Rivera-Velazquez et al., 2021).

El objetivo del presente trabajo fue analizar de manera general la intercomunicación entre controladores a través de sistemas de monitoreo y control que implementen la tecnología

OPC-UA mediante estudios de casos que permitan analizar las características de funcionamiento de la comunicación entre un cliente y servidor. Para esto se realizaron estudios de casos a través de escenarios de simulación variando parámetros propios de cada alternativa, así como parámetros generales como las seguridades, cifrado y firma digital, permitiendo de esta manera determinar las características de cada escenario analizando. Cada uno de los casos de estudio planteados permitieron analizar las características de funcionamiento con relación a las tecnologías existentes en términos de eficiencia, seguridad y costos. El análisis de OPC-UA permitió la comunicación inmediata con los sistemas SCADA y los controladores industriales sin previa configuración, por cuanto la tecnología propuesta puede reemplazar eficientemente al sistema tradicional OPC.

MATERIALES

La Fundación OPC emitió el estándar OPC DA, con el objetivo de resolver los problemas de comunicación de datos de diferentes dispositivos bajo diferentes interfaces y protocolos. Debido a su excelente desempeño OPC DA se ha convertido en un estándar ampliamente aceptado. Sin embargo, OPC DA depende de la tecnología COM y tecnología DCOM de plataforma de Microsoft, lo que dificulta que OPC DA se traslade a otras plataformas. El estándar OPC UA tiene todas las funciones de estándar OPC clásico y es independiente de la plataforma Microsoft. Se puede desarrollar en varios sistemas y dispositivos embebidos usando C/C++, .NET o pila de software Java, y demás ventajas en rendimiento de seguridad y espacio de direcciones integrados, además incluye servicios como: conectarse a servidores, leer/escribir, suscribir y métodos de llamada. Convirtiéndose en un sistema económico y flexible de usar (Krylova et al., 2021; Ren et al., 2019). El sistema de comunicación OPC UA brinda una mejor funcionalidad que el sistema OPC tradicional ya que es difícil de simular en sistemas operativos que no sean de Microsoft, sistemas basados en la arquitectura Microsoft COM/DCOM. También tiene su propio modelo de seguridad combinado al de las propias seguridades de las unidades interconectadas al servicio OPC tradicionales. Sin embargo, la arquitectura OPC UA permite cada vez más interconexiones a dispositivos en IoT, considerando que cada vez están aumentando las cargas generales de la red por la

utilización de más dispositivos y a medida que la velocidad de procesamiento se vuelve más rápida. (Lai et al., 2020). En (Adlok & Nikam, 2017) se realizan pruebas en un emulador de controladores de accionamientos de medio voltaje utilizando una interfaz de tecnología OPC, que ha permitido realizar operaciones como iniciar y detener, así como proporcionar una velocidad de referencia o par al variador emulado. En este trabajo se ha logrado determinar que la tecnología OPC puede ser aplicada en un escenario real donde las señales de control las de una unidad externa y que las mismas pueden gestionarse a través de interfases con tecnología OPC permitiendo de esta manera demostrar la ventaja del uso de esta nueva tecnología en relación a las utilizadas actualmente en estos procesos.

Existen algunos estudios presentados que prueban la aplicabilidad de la comunicación OPC-UA y que fueron tomados en consideración. La eficiencia de la comunicación OPC-UA con 4 diferentes maneras de comunicación fueron comparadas en base a diferentes escenarios como son la comunicación con el nivel empresarial, con sistemas HMIs, entre controladores industriales y con dispositivos de campo. Cada escenario fue evaluado con respecto al tiempo de ciclo y latencia, precisión de tiempo de sincronismo, número de subscriptores, requerimientos de hardware, dificultad de configuración y QoS. Los resultados de esta evaluación nos dan un indicativo que a nivel empresarial y de Sistemas Hombre Maquina (HMI), el más adecuado es el modo Servidor/Cliente de la tecnología OPC-UA y que justifica su mayor análisis (Eckhardt et al., 2018).

MÉTODOS

A través de máquinas virtuales se simuló la comunicación OPC-UA entre cliente y servidor. Los datos seleccionados fueron del tipo doble variando la cantidad entre 5 – 1000. Con la captura de datos por medio del software "WireShark", se observó y estimo el ancho de banda (AB) utilizado por el protocolo de comunicación. También se empleó diferentes políticas de seguridad, visualizando su comportamiento para realizar un análisis comparativo. Adicionalmente se variaron los periodos de muestreo en el intercambio de datos para comparar el uso del AB. Finalmente, se validó un escenario experimental con el Cliente OPC-UA ejecutándose en Windows Server y en Linux Ubuntu con el fin de corroborar la

autonomía del protocolo en distintos sistemas operativos. En la Tabla 1 se detallan los equipos utilizados para los ensayos.

Tabla 1: Computadoras y dispositivos de red usados en los experimentos y pruebas.

Equipos	Uso
Laptop HP ProBook 4730s, con procesador Intel Core i7 de 2.2 MHz, con 8Gb de memoria RAM y sistema operativo Windows 10 de 64 bits. Instalado el software para manejo de máquinas virtuales "VirtualBox" versión 5.0.20	Computador portátil para la simulación del servidor OPC UA seleccionado y del sistema SCADA.
Laptop Dell Inspiron M531R-5535 con procesador AMD A8 de 1.7 MHz, con 6 Gb de memoria RAM y sistema operativo Windows 10 de 64 bits. Instalado el software para manejo de máquinas virtuales "VirtualBox" versión 5.0.20	Computador portátil para la simulación del servidor OPC UA seleccionado y del controlador industrial basado en PC
Switch de datos TP-LINK TL-SG105E de 5 puertos de red Gigabit Ethernet	Switch de datos con funcionalidad de port mirroring para el monitoreo de tráfico de datos.
Red LAN privada	Red LAN privada para la comunicación entre los computadores portátiles de prueba

Fuente: *propia.*

En la Tabla 2 se observan las configuraciones de hardware de las máquinas virtuales y el respectivo uso en los escenarios de prueba.

Tabla 2. Configuración y uso de las máquinas virtuales usadas en las diferentes pruebas.

Máquinas virtuales en Laptop HP Probook 4730s	Uso
Máquina virtual con 2 microprocesadores, 2 Gb de memoria y 60 Gb de disco duro virtual, con sistema operativo Windows Server 2012 R2 a 64 bits.	Máquina virtual utilizada para la ejecución del servidor OPC UA seleccionado
Máquina virtual con 2 microprocesadores, 2 Gb de memoria y 60 Gb de disco duro virtual, con sistema operativo Windows Server 2008 R2 a 64 bits.	Máquina virtual utilizada para la ejecución del sistema SCADA seleccionado

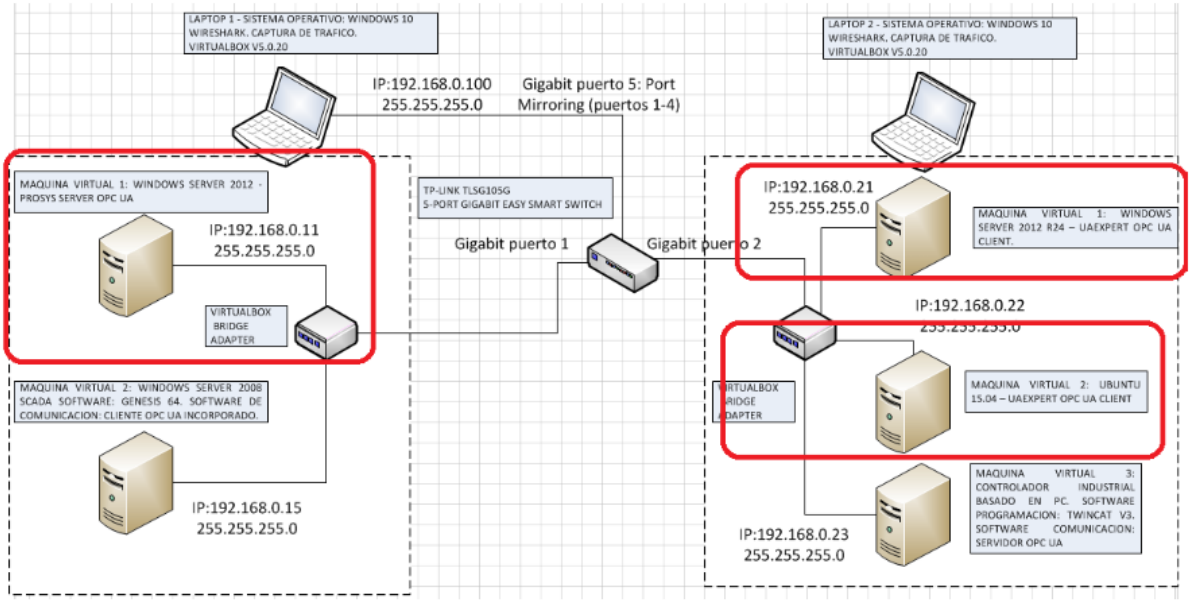
ISSN:2806-5875
Correo: revista@ister.edu.ec

Máquinas virtuales en Laptop Dell Inspiron M531R	Uso
Máquina virtual con 2 microprocesadores, 2 Gb de memoria y 60 Gb de disco duro virtual, con sistema operativo Windows Server 2012 R2 a 64 bits.	Máquina virtual utilizada para la ejecución del servidor OPC UA seleccionado en sistema operativo Windows.
Máquina virtual con 2 microprocesadores, 2 Gb de memoria y 60 Gb de disco duro virtual, con sistema operativo Linux versión Ubuntu 14.04 LTS a 64 bits.	Máquina virtual utilizada para la ejecución del servidor OPC UA seleccionado en sistema operativo Linux.
Máquina virtual con 2 microprocesadores, 2 Gb de memoria y 60 Gb de disco duro virtual, con sistema operativo Windows 7 a 32 bits.	Máquina virtual utilizada para la ejecución del controlador industrial basado en PC.

Fuente: *propia.*

La Fig. 1 muestra la topología de la red LAN local utilizada en las pruebas.

Fig. 1. Topología de la red LAN para las pruebas.



Fuente: *propia.*

Selección de clientes OPC-UA para las respectivas pruebas.

La Tabla 3 indica una comparación de las características de los clientes OPC-UA revisados.

ISSN:2806-5875
Correo: revista@ister.edu.ec

Tabla 3. Comparación de las características de clientes OPC-UA para las pruebas.

Cliente OPC	Sistema Operativo soportado	Exploración de datos	Interfaz gráfica	Lenguaje SDK	Configuración del tiempo de muestreo de las variables OPC	Cambio del número de variables OPC leídas
Prosys	Windows, Linux, MAC OS	Datos básicos, Estructuras	Si	Java	Fijo (1000 ms)	Si
UaExpert	Windows, Linux,	Datos básicos, Estructuras	Si	C++	Variable (desde 100 ms)	Si
OPC Foundation	Windows	Datos básicos, Estructuras	Si	.NET	Variable (desde 1000 a 5000 ms)	Número Limitado

Fuente: *propia.*

Selección de servidores OPC-UA para las respectivas pruebas.

De la misma manera, en la Tabla 4, se muestra una comparación de las características de los servidores OPC UA para las pruebas y poder seleccionar el más adecuado.

Tabla 4. Comparación de características de servidores OPC-UA.

Servidor OPC	Sistema Operativo soportado	Presentación de datos	Interfaz gráfica	Lenguaje SDK	Visor y configuración de modos y políticas de seguridad	Visor de eventos de conexión entre servidor y cliente	Cambio del tiempo de publicación de variables OPC	Herramienta de configuración de permisos de usuarios
Prosys	Windows, Linux, MAC OS	Datos básicos, Estructuras	Si	Java	Visor – Configuración	Si (detallado)	Si	Si
Unified Automation ANSI C	Windows, Linux, MAC OS	Datos básicos, Estructuras	No	ANSI C	No	No	No	No

Unified Automation C++	Windows, MAC OS	Datos básicos, Estructuras	No	C++	Visor – Configuración	No	No	Si
OPC Foundation	Windows	Datos básicos, Estructuras	Si	.NET	Visor – Configuración	Si (básico)	No	No

Fuente: *propia.*

Selección del cliente y del servidor OPC-UA.

Después de un análisis comparativo de las características funcionales se determinó como la mejor alternativa al cliente que cuenta con interfaz gráfico y de monitoreo en línea de variables OPC-UA, por lo cual para el presente trabajo se seleccionó el cliente desarrollado por Unified Automation, Adicionalmente el mismo se ejecuta tanto en Windows como en Linux. Para la selección del Servidor OPC-UA se validó que cuente con interfaz gráfica de fácil utilización y monitoreo de usuarios conectados. El servidor que cumple con estas características fue el desarrollado por Prosys.

Escenario de prueba

Los datos del tipo doble de 32 bits son los más empleados en variables industriales, debido a esto fueron los más idóneos para la ejecución de las pruebas. Se realizó también la lectura de estructura de datos utilizados en aplicaciones específicas. Se capturaron paquetes del proceso de lectura de las variables en un tiempo de muestreo. En las pruebas iniciales no se contempló ningún modo de seguridad (no estuvieron firmados ni encriptados), subsiguientemente se validó los demás modos de seguridad y políticas, evidenciando el comportamiento del consumo de AB. El primer escenario de prueba empieza con la suscripción y lectura de 5 variables con un tiempo de muestreo de 1 segundo. Luego, se realizan otros escenarios de prueba en los cuales se van aumentando la suscripción de las variables a leer, desde 5 variables a 1000, utilizando el mismo tiempo de muestreo con el objetivo de observar el comportamiento del proceso de lectura y la comunicación al aumentar el número de las variables. Además, se realizaron más escenarios de prueba en los cuales se redujo el tiempo de muestreo desde un valor de 1 segundo hasta 100 mili-segundos, y de igual forma, observar

el comportamiento del proceso de lectura de las variables al reducir el tiempo de muestreo. Para validar la interoperabilidad del protocolo de comunicación y comparar el funcionamiento de OPC – UA en diferentes sistemas operativos, se instaló el cliente OPC-UA llamado UaExpert en dos diferentes sistemas operativos como son Windows Server y Linux Ubuntu, y se realizaron pruebas de comunicación con el protocolo. Finalmente, se probaron los modos de seguridad disponibles en el cliente OPC-UA como son: la autenticación anónima, con usuario y clave, y con certificados digitales.

RESULTADOS Y DISCUSIÓN

Resultados del proceso de lectura de datos sin firma digital y sin encriptado

De los datos obtenidos con la captura de paquetes en red, se puede estimar el ancho de banda de petición de datos desde el cliente al servidor OPC UA y el ancho de banda de la correspondiente respuesta. En las respectivas pruebas, se incrementa el número de datos y se puede observar que se incrementan la segmentación de paquetes con lo cual se incrementa el ancho de banda. Al emplear autentificación de la contraseña y del usuario, presenta en este caso, aumento de paquetes debido a que se trasmite el certificado o contraseña y presenta alteración de ancho de banda. Esto se puede corroborar en la Tabla 5.a y 5.b.

Tabla 5.a. Cuadro comparativo de las pruebas de lectura de datos sin firma digital y sin encriptado.

Escenario de prueba	Modo de Seguridad	Política de Seguridad	Autenticación de Usuario	t de muestreo [ms]	Núm. de datos (Tipo doble)	Núm. de segmentos del paquete	Núm. de peticiones por segundo	Núm. de bytes por datos
Prueba 1	Ninguno	Ninguno	Anónimo	1000	5	1	1	150
				1000	11	1	1	330
				1000	51	2	1	1530
				1000	1000	21	1	30000
Prueba 2	Ninguno	Ninguno	Anónimo	500	1000	21	2	30000
Prueba 3	Ninguno	Ninguno	Anónimo	100	1000	21	10	30000

ISSN:2806-5875
Correo: revista@ister.edu.ec

Prueba 4	Ninguno	Ninguno	Anónimo	100	1000	21	10	30000
Prueba 5	Ninguno	Ninguno	Anónimo	100	1000	21	10	30000

Fuente: *propia.*

Tabla 5.b. Cuadro comparativo del ancho de banda capturado en las pruebas de lectura de datos sin firma digital y sin encriptado.

Escenario de prueba	**AB (Petición lectura de datos) [bps]**	**AB (Respuesta lectura de datos) [bps]**	**AB (Respuesta estado del servidor) [bps]**	**AB (Respuesta a estado del servidor) [bps]**	**AB total (Petición datos y estado servidor) [bps]**	**AB total (respuesta de datos y estado de servidor) [bps]**	**Observaciones**
Prueba 1	1504	3088	1680	2680	3184	5768	Contraseña o certificado enviado únicamente en la activación de la sesión, más no en los datos
	1504	4528	1680	2680	3184	7208	
	1504	14560	1680	2680	3184	17240	
	1504	251104	1680	2680	3184	253784	
Prueba 2	3008	502208	1680	2680	4688	504888	
Prueba 3	15040	2511040	1680	2680	16720	2513720	
Prueba 4	15040	2511040	1680	2680	16720	2513720	
Prueba 5	15040	2511040	1680	2680	16720	2513720	

Fuente: *propia.*

Resultados de las pruebas de lectura de datos con firma digital y sin encriptado

En estos escenarios, a consecuencia de la firma digital, se adicionan 20 bytes extras al final de cada solicitud y respuesta de los datos, esto causa el aumento del ancho de banda, aun en el caso de emplear segmentos de paquete que posee la firma digital al final del paquete. Esto se puede corroborar en la Tabla 6.a y Tabla 6.b.

Tabla 6.a. Cuadro comparativo de las pruebas con lectura de datos con firma digital y sin encriptado.

Escenario de prueba	Modo de Seguridad	Política de Seguridad	Autenticación de Usuario	t de muestreo [ms]	Núm. de datos	Núm. de segmentos del paquete	Núm. de peticiones por segundo	Núm. de bytes por datos
Prueba 6	Mensaje firmado	Basic 128RSA15	Anónimo	1000	6	1	1	180
				1000	100	3	1	3000
Prueba 7	Mensaje firmado	Basic 128RSA15	Anónimo	500	100	3	2	3000
Prueba 8	Mensaje firmado	Basic 128RSA16	Anónimo	100	100	3	10	3000
Prueba 9	Mensaje firmado	Basic 256	Anónimo	1000	100	3	1	3000
Prueba 10	Mensaje firmado	Basic 256	Anónimo	500	100	3	2	3000
Prueba 11	Mensaje firmado	Basic 256	Anónimo	100	100	3	10	3000
Prueba 12	Mensaje firmado	Basic 256SHA256	Anónimo	100	100	3	10	3000

Fuente: *propia.*

ISSN:2806-5875
Correo: revista@ister.edu.ec

Tabla 6.b. Cuadro comparativo del ancho de banda capturado de la lectura de datos con firma digital y sin encriptado.

Escenario de prueba	AB (Petición lectura de datos) [bps]	AB (Respuesta lectura de datos) [bps]	AB (Respuesta estado del servidor) [bps]	AB (Respuesta estado del servidor) [bps]	AB total (Petición datos y estado servidor) [bps]	AB (Respuesta datos y estado servidor) [bps]	Observaciones
Prueba 6	1664	3488	1840	2840	3504	6328	Difiere en 20 bytes en la petición y la respuesta de lectura de datos debido a la firma digital
	1664	26912	1840	2840	3504	29752	
Prueba 7	3328	53824	1840	2840	5168	56664	
Prueba 8	16640	269120	1840	2840	18480	271960	
Prueba 9	1664	26912	1840	2840	3504	29752	
Prueba 10	3328	53824	1840	2840	5168	56664	
Prueba 11	16640	269120	1840	2840	18480	271960	
Prueba 12	17600	269760	1840	2840	19440	272600	

Fuente: *propia.*

Resultados de las pruebas de lectura de datos con firma digital y encriptado

En estos escenarios no se presentó incremento notorio en el ancho de banda empleado en comparación a la lectura de datos que utilizan una firma digital. Presenta una gran diferencia con respecto al tiempo de ida y vuelta de los mensajes de los datos con un incremento del doble, esto se demuestra en la Tabla 7.a y Tabla 7.b.

Tabla 7.a. Cuadro comparativo de las pruebas de lectura de datos con firma digital y encriptado.

Escenario de prueba	Modo de Seguridad	Política de Seguridad	Autenticación de usuario	Tiempo de Muestreo [ms]	Núm. datos	Núm. de segmentos del paquete	Núm. de peticiones por segundo	Núm. de bytes por datos
Prueba 13	Mensaje firmado y cifrado	Basic128RSA15	Anónimo	1000	100	3	1	3000

Prueba 14	Mensaje firmado y cifrado	Basic128RSA15	Anónimo	500	100	3	2	3000
Prueba 15	Mensaje firmado y cifrado	Basic128RSA15	Anónimo	100	100	3	10	3000
Prueba 16	Mensaje firmado y cifrado	Basic256	Anónimo	100	100	3	10	3000
Prueba 17	Mensaje firmado y cifrado	Basic128RSA15	Anónimo	100	100	3	10	3000

Fuente: *propia.*

Tabla 7.b. Cuadro comparativo del ancho de banda capturado en las pruebas de lectura de datos con firma digital y encriptado.

Escenario de prueba	**AB (Petición lectura de datos) [bps]**	**AB (Respuesta lectura de datos) [bps]**	**AB (Respuesta estado del servidor) [bps]**	**AB (Respuesta estado del servidor) [bps]**	**AB total (Petición datos y estado servidor) [bps]**	**AB total (Respuesta datos y estado servidor) [bps]**	**Observaciones**
Prueba 13	1680	26992	1840	2840	3520	29832	Aumento del tiempo de ida y retorno de los datos debido al proceso de cifrado
Prueba 14	3360	53984	1840	2840	5200	56824	
Prueba 15	16800	269920	1840	2840	18640	272760	
Prueba 16	16800	269920	1840	2840	18640	272760	
Prueba 17	16800	269920	1840	2840	18640	272760	

Fuente: *propia.*

Resultados de las pruebas de lectura de datos con firma digital y encriptado con simulación SCADA.

Se pueden notar las diferencias en el ciclo de ida y retorno de los mensajes de los datos, entre los casos de comunicación con política de seguridad Basic128Rsa15 y el caso con política de seguridad Basic256, en que se puede percibir un incremento notorio por el procesamiento

de encriptado y desencriptado, y la administración de reorganización de datos entre estos casos de comunicación, esto se demuestra en la Tabla 8.a y Tabla 8.b.

Tabla 8.a. Cuadro comparativo de las pruebas de lectura de datos con firma digital y encriptado de la simulación SCADA.

Escenario de prueba	Modo de seguridad	Política de seguridad	Autenticación de usuario	t de muestreo [ms]	Núm. de datos	Núm. De segmentos del paquete	Núm. De peticiones por seg.	Núm. De bytes por datos
Prueba 18	Mensaje sin firmado y cifrado	Ninguno	Anónimo	100	32	1	10	256
Prueba 19	Mensaje sin firmado y cifrado	Basic128RSA15	Anónimo	100	32	1	10	256
Prueba 20	Mensaje sin firmado y cifrado	Basic256	Anónimo	100	32	1	10	256

Fuente: *propia.*

Tabla 8.b. Cuadro comparativo del ancho de banda utilizado de las pruebas de lectura de datos con firma digital y encriptado de la simulación SCADA.

Escenario de prueba	AB (Petición lectura de datos) [bps]	AB (Respuesta lectura de datos) [bps]	AB (Respuesta estado del servidor) [bps]	AB (Respuesta estado del servidor) [bps]	AB total (Petición datos y estado servidor) [bps]	AB total (Respuesta datos y estado servidor) [bps]	Observaciones
Prueba 18	10240	35680	0	0	10240	35680	Aumento del tiempo de ida y retorno de los datos debido al
Prueba 19	12000	37600	0	0	10240	37600	

Prueba 20	12000	37600	0	0	10240	37600	proceso de cifrado y manejo de arreglos.

Fuente: *propia.*

Estos datos presentados en los diferentes escenarios indica, dependiendo del tipo de escenario, que podemos reducir el ancho de banda.

Es conveniente emplear como cliente OPC UA al programa "UAExpert", porque tiene una interfaz visual más detallada que incluye ventanas de monitoreo y facilita el añadir las variables OPC UA desde la ventana de espacio de direcciones hasta las vistas de subscripciones de la interfaz. También nos permite trabajar en el sistema operativo como Windows o en Linux.

TRABAJOS FUTUROS

Se realizará un análisis de tipos de controladores industriales y su interoperabilidad con diferentes sistemas operativos, así como su flexibilidad para soporte de envió de datos a diferentes protocolos de comunicación orientados a industria 4.0.

CONCLUSIONES

El uso del sistema de comunicación OPC-UA redujo las complejidades de configuración ya que soporta sistemas abiertos, toleró cortafuegos y la configuración es por puertos definidos adecuados ya que no genera puertos aleatorios.

Las reducciones del ancho de banda que se producen con el uso de OPC-UA dependieron del periodo de muestreo, de la cantidad de mensajes y del tipo de datos. Los datos verificados fueron del tipo doble con un tiempo de muestreo de 10 a 10000 milisegundos sin encriptado. Para el sistema de comunicación OPC-UA se recomienda utilizar datos del tipo doble del tipo entero para disminuir tamaño de bytes, aunque con los de tipo decimal se gana en precisión, con tiempos de muestreo rápido para información crítica y tiempos lentos para información no crítica.

La comunicación OPC-UA permitió la validación inmediata de variables desde el sistema SCADA hasta los controladores industriales sin previa configuración, lo que demuestra que el sistema de comunicación OPC-UA puede reemplazar eficazmente al sistema tradicional OPC.

REFERENCIAS

Adlok, N., & Nikam, A. (2017). Automatic testing of medium voltage drive using OPC server interface. *2017 International Conference on Smart grids, Power and Advanced Control Engineering (ICSPACE)*, 65-68. https://doi.org/10.1109/ICSPACE.2017.8343407

Almeida, C. (s. f.). Unified Architecture. *OPC Foundation*. Recuperado 30 de junio de 2022, de https://opcfoundation.org/about/opc-technologies/opc-ua/

Drahoš, P., Kučera, E., Haffner, O., & Klimo, I. (2018). Trends in industrial communication and OPC UA. *2018 Cybernetics & Informatics (K&I)*, 1-5. https://doi.org/10.1109/CYBERI.2018.8337560

Eckhardt, A., Müller, S., & Leurs, L. (2018). An Evaluation of the Applicability of OPC UA Publish Subscribe on Factory Automation use Cases. *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, *1*, 1071-1074. https://doi.org/10.1109/ETFA.2018.8502445

Eymüller, C., Hanke, J., Hoffmann, A., Kugelmann, M., & Reif, W. (2020). Real-time capable OPC-UA Programs over TSN for distributed industrial control. *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, *1*, 278-285. https://doi.org/10.1109/ETFA46521.2020.9212171

Germany, B. A. G. & C. K., Hülshorstweg 20, 33415 Verl. (s. f.). *Beckhoff New Automation Technology*. Beckhoff Automation. Recuperado 30 de junio de 2022, de https://www.beckhoff.com/es-es/

Han, D., Gong, Y., & Xu, D. (2022). Research on Key Technologies of OPC UA Standard and Test. *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, 95-98. https://doi.org/10.1109/IPEC54454.2022.9777611

Krylova, E. L., Nemudruk, M. L., Shchurov, D. A., Novozhilov, I. M., & Fedorov, M. S. (2021). The Use of OPC UA Technology in the Study of Models of Control Objects. *2021 IV International Conference on Control in Technical Systems (CTS)*, 171-173. https://doi.org/10.1109/CTS53513.2021.9562917

Lai, Y. H., Huang, Y.-H., Lai, C. F., Chen, S. Y., & Chang, Y.-C. (2020). Dynamic Adjustment Mechanism based on OPC-UA Architecture for IIoT Applications. *2020 Indo – Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN)*, 335-338. https://doi.org/10.1109/Indo-TaiwanICAN48429.2020.9181337

Marksteiner, S. (2018). Reasoning on Adopting OPC UA for an IoT-Enhanced Smart Energy System from a Security Perspective. *2018 IEEE 20th Conference on Business Informatics (CBI)*, *02*, 140-143. https://doi.org/10.1109/CBI.2018.10060

Muennoi, A., & Hormdee, D. (2016). 3D Web-based HMI with WebGL Rendering Performance. *MATEC Web of Conferences*, *77*, 09003. https://doi.org/10.1051/matecconf/20167709003

Okuda, M., Mizuya, T., & Nagao, T. (2017). Development of IoT testbed using OPC UA and database on cloud. *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 607-610. https://doi.org/10.23919/SICE.2017.8105726

OPC UA_test. (s. f.). Recuperado 3 de julio de 2022, de https://page.advantech.com/opc-ua-test

Ren, H., Liu, Y., & Wang, H. (2019). Research on Communication Method of OPC UA Client Based on ARM. *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*, 52-56. https://doi.org/10.1109/ICIS46139.2019.8940214

Rivera-Velazquez, F., Salazar-Valle, E., & Martínez-Águilar, G. M. (2021). OPC UA server on Raspberry Pi and Arduino for didactic use. *2021 10th International Conference On Software Process Improvement (CIMPS)*, 115-124. https://doi.org/10.1109/CIMPS54606.2021.9652694

Schwarz, M. H., & Börcsök, J. (2013). A survey on OPC and OPC-UA: About the standard, developments and investigations. *2013 XXIV International Conference on Information, Communication and Automation Technologies (ICAT)*, 1-6. https://doi.org/10.1109/ICAT.2013.6684065

Yuan, H., Hao, H., & Zhang, M. (2021). Overview of OPC UA TSN. *2021 IEEE 5th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC)*, *5*, 715-718. https://doi.org/10.1109/ITNEC52019.2021.9586911