RIELAC
Revista de Ingeniería Electrónica, Automática y Comunicaciones

Sistema para la supervisión de indicadores productivos y tecnológicos en la Planta Cloro-Sosa ELQUIM

Marcel Mesa Martínez, Miguel Luis Sojo Hernández, Guillermo Ámbar Pérez, Ivan Santana Ching

RESUMEN / ***ABSTRACT***

Tradicionalmente, los Sistemas de Control Industrial han estado aislados en redes privadas y altamente seguras. Sin embargo, en los últimos años ha surgido una tendencia hacia la integración de estos sistemas con Internet, buscando facilitar el intercambio de datos fundamentales para la gestión empresarial y la toma de decisiones precisas en el ámbito de la producción. Este movimiento hacia la convergencia con Internet plantea desafíos significativos en el ámbito de la ciberseguridad. La empresa Electroquímica (ELQUIM) de Sagua la Grande implementó recientemente una nueva planta más productiva y segura. Un Sistema de Control Industrial supervisa y controla los parámetros productivos y tecnológicos de la planta, sin embargo, no existía un mecanismo de recolección y almacenamiento de los mismos desde la zona empresarial. Se diseñó un sistema para la adquisición de forma segura de los datos de la zona de procesos y colocarlos disposición de los especialistas y tecnólogos en la zona empresarial. A través de esta información los tecnólogos pueden detectar un mal funcionamiento de la planta, así como mejorar los procesos productivos de la misma. Como software de supervisión fue utilizado el SCADA ErosXD diseñado y programado por las empresas SERCONI y XETID.

Palabras claves: Sistemas de Control Industrial (ICS); Cortafuegos; SCADA; Supervisión; Ciberseguridad

Traditionally, Industrial Control Systems have been isolated in private and highly secure networks. However, in recent years a trend has emerged towards the integration of these systems with the Internet, seeking to facilitate the exchange of fundamental data for business management and making precise decisions in the field of production. This movement towards convergence with the Internet poses significant challenges in the field of cybersecurity. The Electrochemical company (ELQUIM) of Sagua la Grande recently implemented a new, more productive and safer plant. An Industrial Control System supervises and controls the productive and technological parameters of the plant, however, there was no mechanism for collecting and storing them from the business area. A system was designed to securely acquire data from the process area and place it at the disposal of specialists and technologists in the business area. Through this information, technologists can detect malfunctions in the plant, as well as improve its production processes. The SCADA ErosXD designed and programmed by the companies SERCONI and XETID was used as supervision software.

Keywords: Industrial Control System (ICS); Firewall; SCADA; Supervision; Cybersecurity

System for the supervision of productive and technological indicators in the ELQUIM Chlorine-Soda Plant

1. -INTRODUCCIÓN

Los Sistemas de Control Industrial (ICS) incluyen en su definición a los sistemas de Supervisión, Control y Adquisición de Datos (SCADA), a los Sistemas de Control Distribuido (DCS) y a otras configuraciones de sistemas de control, como los controladores lógicos programables (PLC) [1]. Los ICS suelen ser usados en los sectores industriales y las Infraestructuras Críticas, como las plantas nucleares y térmicas, las instalaciones de tratamiento de agua, la generación de energía, las industrias químicas, las industrias pesadas y los sistemas de distribución [2]. Durante varios años los ICS se mantuvieron aislados de Internet, manteniendo su integridad a través de la seguridad por oscuridad y mediante protocolos especialmente

Recibido: 01/2023 Aceptado: 04/2023

diseñados para la industria [3]. Sin embargo, los importantes beneficios empresariales que se alcanzan promueven una convergencia entre los ICS e Internet, en especial la computación en la nube e IoT [4]. Como resultado de este vínculo, los ICS han estado expuestos a los ciberataques [5]. Los dispositivos ICS son mucho menos seguros contra tales escenarios de ataque avanzados que los sistemas computacionales tradicionales. Comprometer la seguridad de los ICS puede conducir a enormes daños físicos y un posible peligro para la vida humana [6].

Desde hace varias décadas los expertos han advertido sobre las desastrosas potencialidades que tendría un ataque cibernético a gran escala contra Infraestructuras Críticas vulnerables. En 1991 el experto en seguridad Winn Schwartau definió el término "Electronic Pearl Harbor" y desde esa época son varias las acciones tomadas para evitar posibles ciberataques [7]. Los estados han prestado atención a definir estrategias de ciberseguridad, en especial para las Infraestructuras Críticas [8].

En Cuba se han establecido un conjunto de normativas relacionadas con la ciberseguridad entre las que destaca el Decreto-Ley 370 sobre la "Informatización de la Sociedad en Cuba" que regula la capacidad del Estado para identificar las Infraestructuras Críticas [9]. Por su parte, en el Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" se definen los criterios y las directivas para la protección de las Infraestructuras Críticas [10].

Cuba cuenta con una sola planta de producción de cloro líquido, la Cloro-Sosa de la empresa Electroquímica (ELQUIM), ubicada en el municipio Sagua la Grande. Esta empresa produce además hipoclorito de sodio, sosa cáustica, hidrógeno, sulfato de aluminio y silicatos de sodio líquidos. Recientemente entró en funcionamiento una nueva planta, con tecnología de membranas, más amigable con el medio ambiente [11].

La planta ELQUIM es controlada a través de un ICS compuesto por un Sistema de Control Distribuido (DCS), un Sistema de Apagado de Emergencia (ESD por sus siglas en inglés, Emergency Stop Devices) y PLC en unidades auxiliares. Para fortalecer la seguridad de los ICS, una solución es implementar una defensa en profundidad mediante la combinación de controles de seguridad que reduzcan el riesgo de los activos que se están protegiendo. Al aplicar múltiples controles sobre el ICS se introducen otras barreras que un atacante debe superar [12]. En este sentido se definió e implementó una estrategia de defensa en profundidad para la protección del ICS de la planta de producción de Cloro-Sosa de la empresa ELQUIM cumpliendo con las reglas nacionales e internacionales [11].

El proveedor de la planta, como parte de la garantía de funcionamiento, requiere una revisión de los parámetros tecnológicos en caso de avería. Igualmente es una necesidad empresarial que los especialistas de ELQUIM puedan analizar los parámetros tecnológicos y productivos actuales e históricos, sin acceder al DCS. El DCS adquirido no cuenta con un sistema de almacenamiento de los datos que pueda ser extraído del mismo. Por tanto, es necesario diseñar un sistema de recolección de datos del DCS que puedan ser almacenados en la red empresarial para su utilización actual y futura.

Este artículo está enfocado en el diseño de un sistema de recolección de datos adquiridos de forma segura desde la red industrial de la planta Cloro-Sosa de la empresa ELQUIM y su almacenamiento y supervisión en la red empresarial. El mismo está organizado de la siguiente manera, primeramente, se definen los criterios de diseño del sistema de adquisición de datos de la red industrial. Luego se presenta el diseño del sistema de almacenamiento mostrando los resultados obtenidos durante el proceso de supervisión de los datos adquiridos en tiempo real de la red industrial. Por último, se emiten algunas conclusiones de interés para este y futuros trabajos.

2.- DISEÑO DEL SISTEMA DE ADQUISICIÓN DE DATOS DE LA RED INDUSTRIAL

La estrategia de defensa en profundidad implementada en la planta Cloro-Sosa de la empresa Electroquímica (ELQUIM) sigue las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST) [11]. Dentro de los elementos de seguridad a seguir se encuentra la separación de redes. Un aspecto fundamental a tener en cuenta en el sistema de adquisición de datos de la red industrial, es que no haya ningún contacto con la red empresarial.

El sistema de recolección de datos permite adquirir la información de la red industrial para su posterior almacenamiento y supervisión en la red empresarial. En el diseño se tuvo en cuenta los requisitos específicos para la seguridad del software. La empresa cuenta en su red industrial con una zona de procesos donde están localizados los dispositivos de campo y los restantes componentes utilizados para la producción, todos ellos supervisados, controlados y registrados a través del DCS del proveedor Yokogawa. En dicha zona no debe instalarse ningún otro software no definido por el proveedor pues pondría en riesgo la seguridad del sistema y las licencias.

Como parte del diseño del sistema de recolección, se segmenta la red industrial de la red empresarial a través de una zona desmilitarizada (DMZ). Esta zona se conforma por 2 parejas de cortafuegos (FW) y un servidor que servirá de pasarela para la salida de los indicadores tecnológicos y productivos que se utilizan en la zona empresarial.

2.1.- DISEÑO DE LA ZONA DESMILITARIZADA (DMZ)

Uno de los elementos fundamentales de la seguridad en el diseño lo constituye la DMZ que aloja al recolector de datos a través del protocolo OPC DA. La DMZ está formada por dos cortafuegos de alta disponibilidad (FW HA) [13]. En la implementación de los cortafuegos se utilizaron Raspberry Pi 3 ejecutando una distribución basada en Linux. Esta estructura de cortafuegos de alta disponibilidad posibilita continuidad de servicio frente a fallas de hardware, permite usar hardware standard para funciones críticas, actualizaciones de software sin interrupción y continuidad del servicio ante caída de uno de los enlaces.

Entre la Zona de Procesos (ZP) y la DMZ se establecen los primeros dos cortafuegos con alta disponibilidad denominados FW1_ZP y FW2_ZP (Figura 1). Estos cortafuegos garantizan el paso de información requerida desde el Servidor OPC-DA hacia un servidor recolector de datos. El uso de un servidor OPC-DA en la red industrial requiere el flujo de información bidireccional (desde la DMZ hacia la zona industrial y viceversa) debido a que se usa el protocolo DCOM para la comunicación entre cliente-servidor.

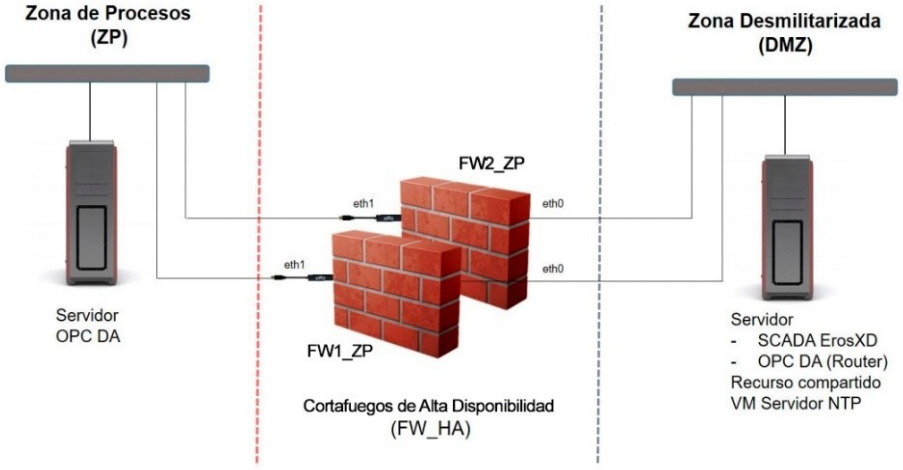

Figura 1.

Cortafuegos de alta disponibilidad ubicados entre la ZP y la DMZ.

Entre la DMZ y la Zona de Gestión (ZG) se ubicaron los otros dos cortafuegos con alta disponibilidad denominados FW1_ZE y FW2_ZE (Figura 2). Estos cortafuegos garantizaron el flujo de información desde la DMZ hacia la red empresarial, tanto para los valores recolectados, como para las configuraciones y datos almacenados en el DCS Yokogawa. En ningún caso debe accederse en sentido contrario.

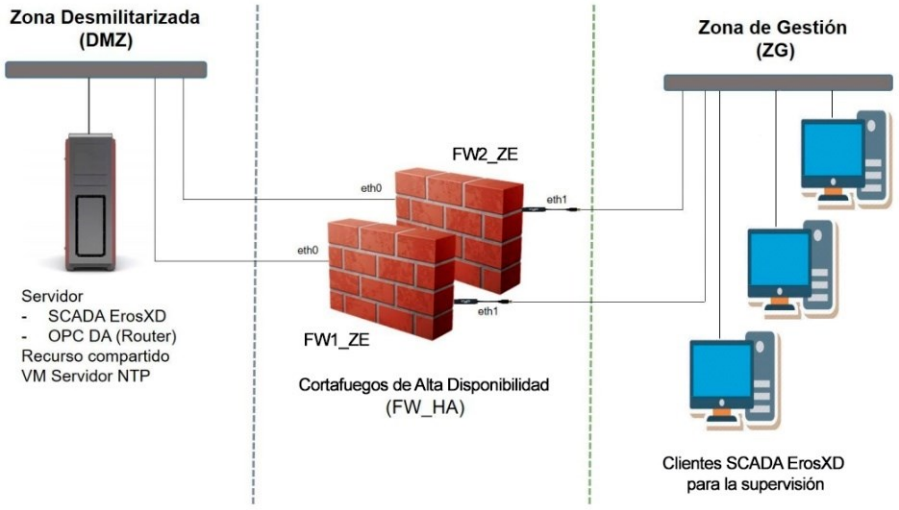

Figura 2.

Cortafuegos de alta disponibilidad ubicados entre la DMZ y la ZG.

3.- DISEÑO DEL SISTEMA DE ALMACENAMIENTO Y SUPERVISIÓN

Uno de los objetivos fundamentales del sistema es el almacenamiento de forma segura de los datos tecnológicos y productivos recolectados desde la zona industrial. Para realizar estas funciones se utiliza un SCADA denominado ErosXD, desarrollado a partir de la colaboración entre las empresas cubanas SERCONI y XETID, sobre la base de la soberanía tecnológica [14].

El SCADA ErosXD es un sistema de supervisión y control de procesos industriales que facilita a los operadores, ingenieros, supervisores y directivos operar y dirigir cualquier proceso con un alto nivel de productividad y eficiencia. Se basa en una arquitectura Cliente/Servidor, formado por una combinación de subsistemas que colaboran entre sí para mostrar al usuario la información necesaria. Para este funcionamiento el Servidor provee a los Clientes de un conjunto de servicios que responden a partir de un pedido mediante los protocolos de comunicación. La interfaz se divide en varios subsistemas, los cuales pueden funcionar de manera independiente sin perder su identidad [14].

En el subsistema configurador el usuario puede definir las características del entorno de trabajo de un proceso industrial. El subsistema recolector constituye la parte más significativa del sistema, es el encargado de la recolección de los datos que se obtienen de los dispositivos externos utilizando los manejadores para su adquisición. El subsistema diseñador permite definir la forma, contenido y estructura de los mímicos a mostrar, así como su relación con cada uno de los elementos configurados previamente en el subsistema configurador. Por último, el subsistema visualizador establece como tarea principal representar a través de los mímicos diferentes áreas de procesos industriales.

3.1.- CARACTERÍSTICAS DEL EROSXD

El SCADA ErosXD es un sistema de supervisión y control de procesos industriales que facilita a los operadores, ingenieros, supervisores y directivos operar y dirigir cualquier proceso con un alto nivel de productividad y eficiencia. Se basa en una arquitectura Cliente/Servidor, formado por una combinación de subsistemas que colaboran entre sí para mostrar al usuario la información necesaria (Figura 3). Para este funcionamiento el Servidor provee a los Clientes de un conjunto de servicios que responden a partir de un pedido mediante los protocolos de comunicación. La interfaz se divide en varios subsistemas, los cuales pueden funcionar de manera independiente sin perder su identidad.

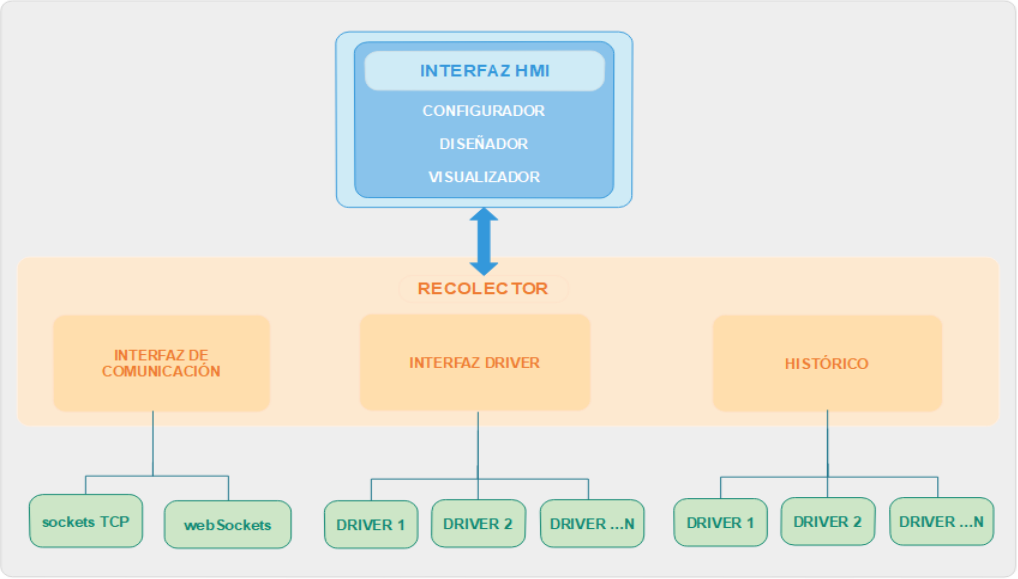

Figura 3.

Arquitectura funcional del SCADA ErosXD. Subsistemas que lo componen

En el **subsistema configurador** el usuario puede definir las características del entorno de trabajo de un proceso industrial. Se realiza de manera jerárquica una representación del conjunto de dispositivos externos que entregarán información al sistema y la configuración de estos. Además, se presentan las características de las variables que el proceso maneja, y se configura el enlace de cada una de ellas con los dispositivos. También se configuran las alarmas asociadas a las variables según las condiciones anormales que ocurran en el proceso industrial. En este subsistema se configuran los usuarios, roles y permisos para el manejo de la seguridad. Todo es representado de manera ordenada en un objeto de control que describe de forma más adecuada el proceso industrial.

El **subsistema recolector** constituye la parte más significativa del sistema, es el encargado de la recolección de los datos que se obtienen de los dispositivos externos utilizando los manejadores para su adquisición. Además, atiende y procesa las peticiones procedentes de los usuarios a través del resto de los componentes del sistema y procesa los valores para el almacenamiento de los datos históricos y los scripts.

El **subsistema diseñador** permite definir la forma, contenido y estructura de los mímicos a mostrar, así como su relación con cada uno de los elementos configurados previamente en el subsistema configurador. Los mímicos son dibujos que representan un área determinada del proceso de control en los cuales se muestra, el estado de los equipos, los valores de las variables, imitaciones de instrumentos o animaciones de los equipos. El objetivo fundamental es mostrar la información que se mide de una manera más rápida, sencilla y agradable a la vista.

Por último, el **subsistema visualizador** establece como tarea principal representar a través de los mímicos diferentes áreas de procesos industriales. Utiliza la colección de variables disponibles en el subsistema configurador para cada dispositivo en el campo. Relaciona las variables con los objetos gráficos representados en los mímicos y de esta forma simula el comportamiento del proceso industrial. Este sistema se encarga de monitorear en tiempo real, los procesos que ocurren en el campo. Se visualizan las alarmas que se activan, se muestra los componentes gráficos implicados, los sensores, las estaciones remotas, y el sistema de comunicación. Todo esto permite al operador estar en contacto directo con el sistema y realizar la supervisión y el control del proceso en general.

3.2.- RECOLECCIÓN DE LAS VARIABLES

Se caracterizaron todas las variables alojadas en el DCS por parte de los especialistas, resultado significativas 640 de ellas. Para la adquisición se configuró el subsistema recolector del ErosXD instalado en la DMZ. Se utilizó como protocolo de comunicación OPC DA. Las variables fueron agrupadas por las unidades en las que se dividen la planta (figura 4).

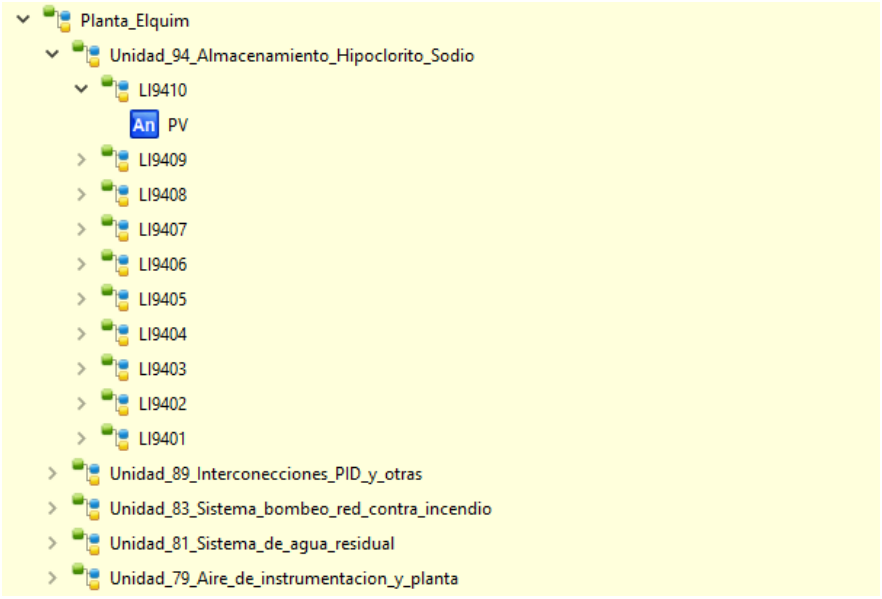

Figura 4.

Arquitectura funcional del SCADA ErosXD. Subsistemas que lo componen.

Se mantuvo el nombre de las variables según son conocidas por los operarios, coincidiendo con la denominación en el DCS. Se realizó una configuración en árbol hasta llegar al valor puntual de la variable. Esto permite la incorporación futura de otras características de las variables como valor máximo, valor mínimo, alarma, etc. La incorporación de los datos sigue una estructura jerárquica.

Las variables recolectadas pueden ser analógicas, discretas, textuales o de tiempo. Las variables adquiridas en este trabajo son analógicas y deben ser correctamente configuradas para su recolección a través del protocolo OPC DA. Las variables siguen un formato que incluye la ubicación en el DCS, el tipo, su función, la unidad dentro de la planta, el número de serie y el valor (Figura 5).

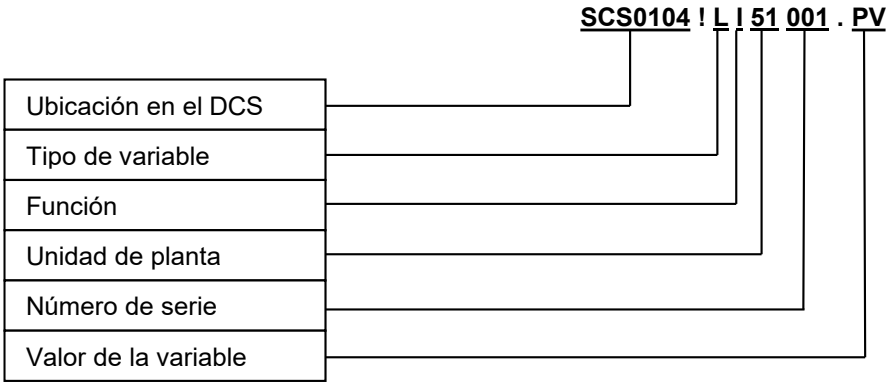

Figura 5.

Formato de las variables adquiridas del DCS Yokogawa

La ubicación en el DCS define en que unidad de control está alojada la variable. El tipo de variable destaca que medición se realiza como: nivel (L), presión (P), presión diferencial (PD), flujo (F), temperatura (T), densidad (D), tensión (U), etc. La función identifica el empleo de la variable, si es de tipo indicador (I), indicador controlador (IC), valor acumulado (YQ), etc. La empresa se divide en diferentes plantas de acuerdo a sus funciones, estas unidades son enumeradas como se mostró anteriormente. Las variables dentro de una unidad son enumeradas a través del número de serie. Por último, las variables tienen diferentes valores como valor puntual (PV), valor alto (HH), valor bajo (LL), si está activa la alarma (ALRM), etc. Los signos de exclamación (!) y el punto (.) dividen las diferentes partes que conforman la estructura de la dirección de las variables. En la tabla 1 se muestran las direcciones de algunas variables importantes.

Tabla 1
Direcciones de variables del proceso

Descripción de la variable	Ubicación en el DCS	Variable del proceso	Función	Unidad de planta	Número de serie	Valor de la variable	Dirección de la variable
Nivel del tanque 51D001	SCS0104	Nivel (L)	Indicador (I)	Síntesis de HCL (51)	001	Valor puntual (PV)	SCS0104!LI51001.PV
Flujo de agua de proceso	FCS0103	Flujo (F)	Indicador (I)	Agua cruda (71)	002	Valor puntual (PV)	FCS0103!FI71002.PV
Temperatura de agua de enfriamiento	FCS0103	Temperatura (T)	Controlador Indicador (IC)	Agua de refrigeración (75)	003	Valor puntual (PV)	FCS0103!TIC75003.PV
Presión en la línea de cloro	FCS0102	Presión (P)	Controlador Indicador (IC)	Celdas (11)	058	Valor puntual (PV)	FCS0102!PIC11058.PV
Concentración de salmuera cruda	FCS0101	Analizador Concentración (A)	Controlador Indicador (IC)	Saturación de salmuera (02)	001	Valor puntual (PV)	FCS0101!AIC02001.PV

La configuración de las variables incluye principalmente las propiedades Generales y el Enlace primario. Dentro de las propiedades Generales está el Dispositivo (1) a través del cual se va a adquirir la variable (OPC para este caso). También se encuentra la Vía de adquisición de la variable (2) (externa para este caso). Algunas Opciones generales (3) como si se habilitan las alarmas, si la variable será de solo lectura, si las estadísticas estarán habilitadas, entre otras. Se incluye la Unidad de medida (4) de la variable adquirida (en el caso del nivel se expresa en %). Por último, se encuentran los Rangos normales de la variable (5), como el rango mínimo, el rango máximo y la banda muerta. Estos valores determinan si se emite una alarma por valor bajo o alto. La banda muerta es el rango a través del cual una entrada puede ser variada sin causar una respuesta medible (Figura 6).

La configuración de la propiedad Enlace primario es fundamental porque incluye el Tiempo de muestreo (1), la Dirección de la variable (2) y el Tipo en dispositivo (3) referente al tipo de dato, entre otras (Figura 7). En la dirección se coloca la ubicación de la variable en el DCS como se mostró anteriormente. La selección del tiempo de muestreo debe ser tenido en cuenta pues un valor muy elevado implicaría la perdida de sucesos importantes, mientras que un valor muy pequeño, almacenaría valores innecesarios.

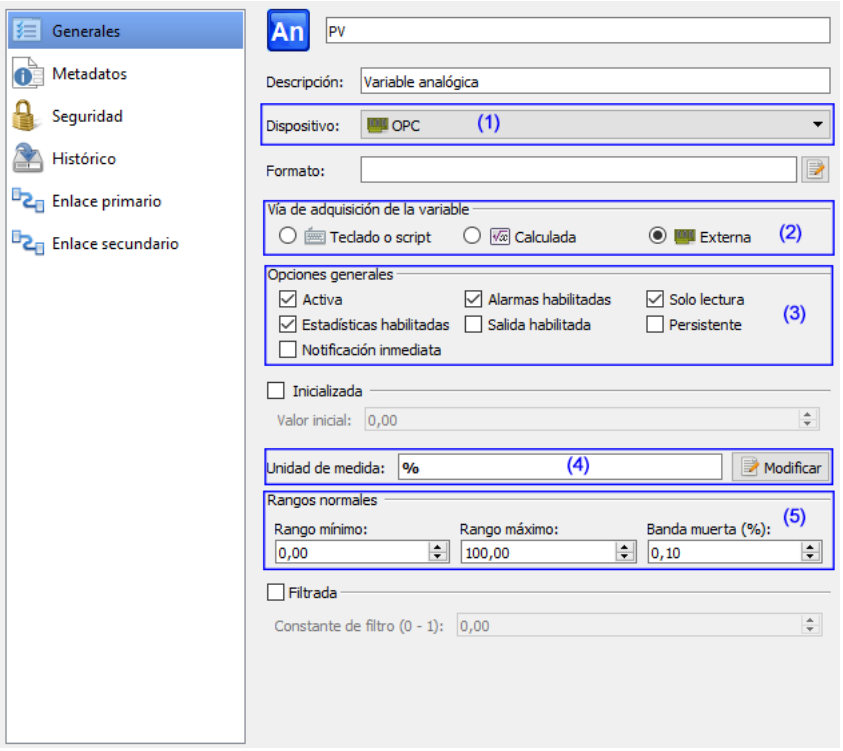

Figura 6

Configuración de la propiedad general de las variables a adquirir

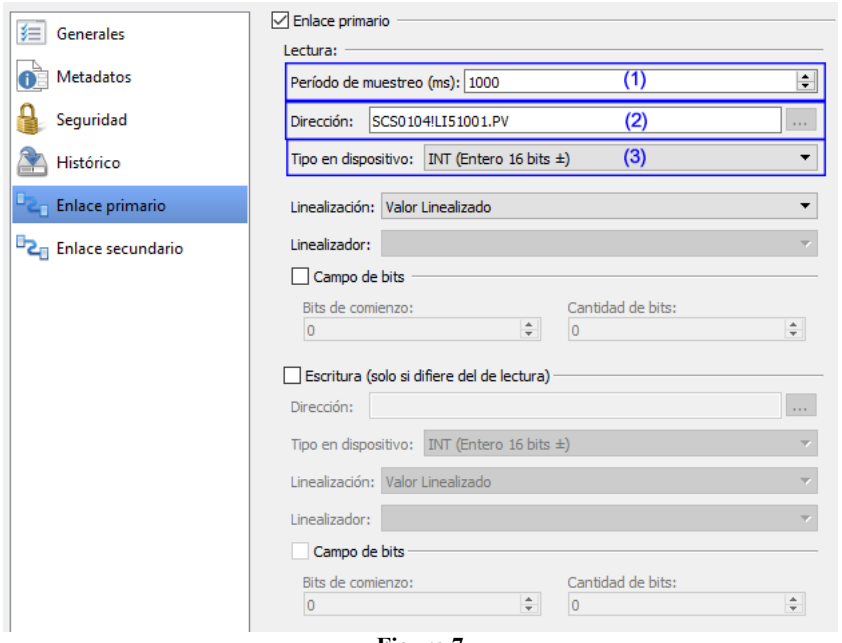

Figura 7

Configuración del enlace primario de las variables a adquirir

3.3.- SUPERVISIÓN DEL SISTEMA

Una vez capturadas correctamente las variables por el recolector, las mismas pueden ser supervisadas a través los mímicos diseñados. Para esto se hace uso de los subsistemas diseñador y visualizador.

Se realizó el diseño de veinte mímicos según el proceso tecnológico que se deseaba representar. La personalización del ErosXD para ELQUIM implicó el diseño de nuevos componentes en la paleta de diseño. Estos componentes quedan para uso futuro en aplicaciones semejantes. En el diseño se tuvo en cuenta la opinión de los operarios de la empresa. Se reflejaron las variables de mayor interés en el proceso productivo por cada una de las áreas. El diseño abarcó entre otras las siguientes unidades: Unidad de agua cruda, Unidad de agua helada, Unidad de enfriamiento, Unidad de agua desmineralizada y almacenamiento, Ventas y Mantenimiento.

Los mímicos diseñados permiten una supervisión de los parámetros productivos fundamentales. Igualmente, se puede revisar el histórico de las variables de interés graficando la tendencia de las mismas. Las variables adquiridas fueron configuradas en los mímicos permitiendo la visualización de sus valores en tiempo real (Figura 8).

La supervisión se realiza desde diversas estaciones incorporadas a la red de gestión. Estas estaciones han sido debidamente aprobadas por la dirección de la empresa y cuentan con los criterios de seguridad definidos.

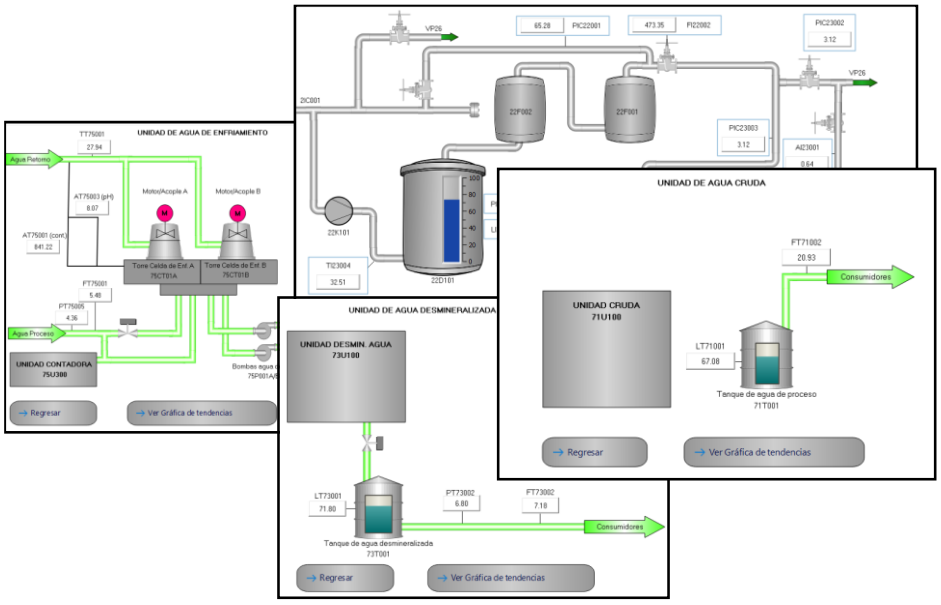

Figura 8.

Supervisión de los procesos productivos.

4.- CONCLUSIONES

El almacenamiento de las variables supervisadas y controladas en el proceso por el DCS constituye un aspecto de vital importancia para el correcto funcionamiento de la planta Cloro-Sosa de la empresa Electroquímica (ELQUIM). Estas variables deben ser almacenadas por un período determinado como parte del plan de seguridad informática y como requisito indispensable por parte del proveedor de la planta para el aseguramiento de la garantía comercial. El DCS adquirido no cuenta con la disponibilidad de almacenar datos, los mismos solo pueden ser consultados en el acceso local.

La adquisición de datos de la zona industrial, a través de cortafuegos de alta disponibilidad y utilizando el protocolo OPC DA, aseguran el almacenamiento de las variables con el período de muestreo requerido.

El uso del software SCADA ErosXD permite la recolección de los datos, así como el almacenamiento en su base datos propia. Esto posibilita la supervisión de parámetros tecnológicos y productivos desde la zona empresarial sin comprometer la seguridad del proceso.

Los mímicos diseñados permiten que especialistas y tecnólogos supervisen el correcto funcionamiento de la planta, así como la producción. De igual forma los directivos, mediante el acceso a reportes adecuados, tomarán decisiones más ágiles y adecuadas en la producción.

REFERENCIAS

1. Plamowski S. Perspectives of DCS and SCADA Systems in High-energy Physics Experiments. Acta Phys Polon Supp. 2018;11:681-4.
2. Lakhoua NM. Review on SCADA Cybersecurity for Critical Infrastructures. Journal of Computer Science and Control Systems. 2017;10(1):15-8.
3. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: A survey. Computers & Security. 2020;89:101677.
4. Brooks T, Chin S-K, editors. Introduction to the Minitrack on Internet of Things Security: CyberAssurance for Edge, Software Defined, and Fog Computing Systems. Proceedings of the 54th Hawaii International Conference on System Sciences; 2021.
5. Alladi T, Chamola V, Zeadally S. Industrial Control Systems: Cyberattack trends and countermeasures. Computer Communications. 2020;155:1-8.
6. Syed D, Chang T-H, Svetinovic D, Rahwan T, Aung Z, editors. Security for Complex Cyber-Physical and Industrial Control Systems: Current Trends, Limitations, and Challenges. PACIS; 2017: AIS eLibrary.
7. Carter W, Sofio D. Cybersecurity Legislation and Critical Infrastructure Vulnerabilities. In: Alperen MJ, editor. Foundations of Homeland Security: Law and Policy. 2nd ed: Wiley; 2017. p. 233-49.
8. Sabillon R, Cavaller V, Cano J. National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering (IJCSSE). 2016;5(5):67-81.
9. Decreto-Ley No. 370/2018. Sobre la Informatización de la Sociedad en Cuba, (4/7, 2019).
10. Decreto No. 360/2019. Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, (4/7, 2019).
11. Socarrás HE, Santana I. Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação. 2019:83-96.
12. Robles-Durazno A, Moradpoor N, McWhinnie J, Russell G, Porcel-Bustamante J. Implementation and Evaluation of Physical, Hybrid, and Virtual Testbeds for Cybersecurity Analysis of Industrial Control Systems. Symmetry. 2021;13(3):519-37.
13. Chen Y, Lee P. An Achievement of High Availability and Low Cost on Data Center Infrastructure. Transactions on Networks and Communications. 2017;5(5):24-38.
14. Benítez-Pina IF. Diseño de un sistema de supervisión y control del centro de datos del Grupo Empresarial CUBANÍQUEL. LADEE. 2022;3(1):1-24.

CONFLICTO DE INTERESES

Ninguno de los autores manifestó la existencia de posibles conflictos de intereses en relación con este artículo.

CONTRIBUCIONES DE LOS AUTORES

Marcel Mesa Martínez: participa en: Conceptualización, Curación de datos, Análisis formal, Investigación, Software, Redacción- borrador original, Redacción – revisión y edición.

Miguel Luis Sojo Hernández participa en: Conceptualización, Curación de datos, Análisis formal, Metodología, Software, Validación -Verificación.

Guillermo Ámbar Pérez participa en: Curación de datos, Análisis formal, Software.

Ivan Santana participa en: Conceptualización, Análisis formal, Adquisición de fondos, Investigación, Metodología, Validación-Verificación, Administración de proyecto, Supervisión, Redacción-borrador original, Redacción – revisión y edición.

AUTORES

Marcel Mesa Martínez: Ingeniero en Ciencias Informática. Empresa de Tecnología e información para la defensa, Habana, Cuba. mmesa@xetid.cu ORCID:0009-0004-0555-6339. Los intereses de investigación están en Machine Learning, IIoT.

Miguel Luis Sojo Hernández: Ingeniero en Ciencias Informática. Empresa de Tecnología e información para la defensa, Habana, Cuba. mlsojo@xetid.cu ORCID: 0009-0007-4334-0039. Los intereses de investigación están en Machine Learning, IIoT.

Guillermo Ámbar Pérez: Ingeniero en Automática. Universidad Central Marta Abreu de Las Villas, Departamento de Control Automático, Villa Clara, Cuba. gambar@uclv.cu ORCID: 0000-0002-1381-4244. Los intereses de investigación están en Sistemas empotrados, sistemas distribuidos, programación, IIoT.

Ivan Santana Ching: Ingeniero en Automática. Doctor en Ciencias Técnicas por la UPM. Universidad Central Marta Abreu de Las Villas, Departamento de Control Automático, Villa Clara, Cuba. ching@uclv.edu.cu ORCID: 0000-0001-5089-520X. Los intereses de investigación están en Sistemas empotrados, Redes de Sensores inalámbricos, Inteligencia Artificial, Machine Learning, IIoT.